Guia do Usuário do Nessus 5.0 Flash

4 de dezembro de 2012

(Revisão 18)

Índice

Introdução

Este documento descreve como usar a **interface do usuário Nessus (UI)** da Tenable Security Network. Envie seus comentários e sugestões para o e-mail support@tenable.com.

A interface do usuário Nessus é uma interface baseada na Web que complementa o scanner de vulnerabilidades Nessus. Para usar o cliente, é preciso um scanner Nessus em operação instalado e estar familiarizado com o seu uso.

Padrões e convenções

Este documento é a tradução de uma versão original em inglês. Algumas partes do texto permanecem em inglês para indicar a representação do próprio produto.

Em toda a documentação, os nomes de arquivos, daemons e executáveis são indicados com a fonte **`courier bold`**, por exemplo, **`gunzip, httpd`** e **`/etc/passwd`**.

As opções de linha de comando e palavras-chaves também são impressas indicadas com a fonte **`courier bold`**. Os exemplos de linhas de comando podem ou não conter o prompt da linha de comando e o texto gerado pelos resultados do comando. Os exemplos de linhas de comando exibirão o comando executado em **`courier bold`** para indicar o que o usuário digitou, enquanto que o exemplo de saída gerado pelo sistema será indicado em `courier` (sem negrito). Um exemplo da execução do comando **`pwd`** do Unix é apresentado a seguir:

```
# pwd
/opt/nessus/
#
```

As observações e considerações importantes são destacadas com este símbolo nas caixas de texto escurecidas.

As dicas, exemplos e práticas recomendados são destacados com este símbolo em branco sobre fundo azul.

Descrição da interface do usuário Nessus

Descrição

A interface do usuário Nessus (UI) é uma interface baseada na Web desenvolvida para o scanner Nessus, que consiste em um servidor HTTP simples e um cliente da Web e dispensa a instalação de qualquer software além do servidor Nessus. A partir do Nessus 4, todas as plataformas aproveitam o mesmo código básico, eliminando a maioria dos erros específicos de plataforma e acelerando a implementação de novos recursos. Os recursos principais são:

- Gera arquivos **`.nessus`** usados pelos produtos da Tenable como padrão de dados de vulnerabilidades e políticas de varredura.
- Uma sessão de política, lista de alvos e os resultados de várias varreduras podem ser armazenados em um único arquivo **`.nessus`**. Consulte o guia de formatos de arquivos do Nessus para obter mais detalhes.
- A interface do usuário exibe, em tempo real, os resultados das varreduras, de modo que não seja preciso esperar a conclusão de uma varredura para ver os resultados.
- Unifica a interface do scanner Nessus, independentemente da plataforma de base. As mesmas funções existem no Mac OS X, Windows e Linux.
- As varreduras continuarão sendo executadas no servidor, mesmo se o usuário for desconectado por qualquer motivo.

- Os relatórios de varredura do Nessus podem ser carregados por meio da interface do usuário Nessus e comparados a outros relatórios.

Plataformas compatíveis

Como a interface do usuário Nessus é um cliente da Web, ela funciona em qualquer plataforma com um navegador.

Para melhor desempenho, a interface do usuário baseada na Web do Nessus deve ser visualizada com o Microsoft Internet Explorer 9, Mozilla Firefox 9.x, Google Chrome 16.x ou Apple Safari 5.x.

Instalação

O gerenciamento do servidor Nessus 5 pelo usuário é realizado por uma interface baseada na Web ou SecurityCenter e dispensa o uso de um NessusClient autônomo. O NessusClient autônomo continua a conectar e operar o scanner, mas deixará de ser atualizado ou oferecer suporte.

Consulte o Guia de Instalação e Configuração do Nessus 5.0 para obter instruções sobre como instalar o Nessus. A partir do Nessus 5.0, Oracle Java (conhecido como Java da Sun Microsystems) é necessário para a funcionalidade de relatórios no formato PDF.

Operação

Visão geral

O Nessus oferece uma interface simples, mas poderosa, para gerenciar as atividades de varredura de vulnerabilidades.

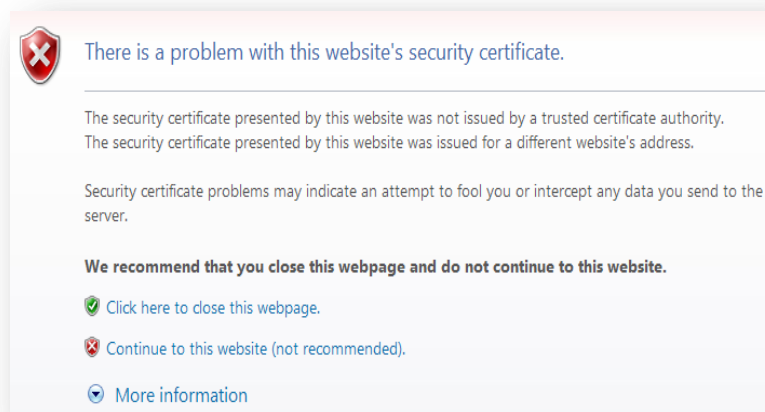
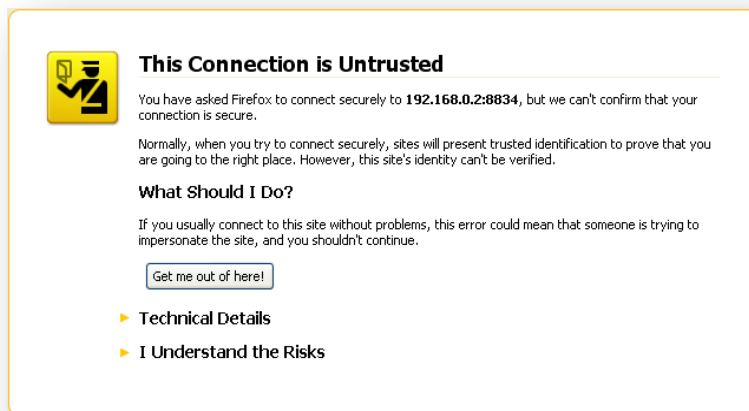
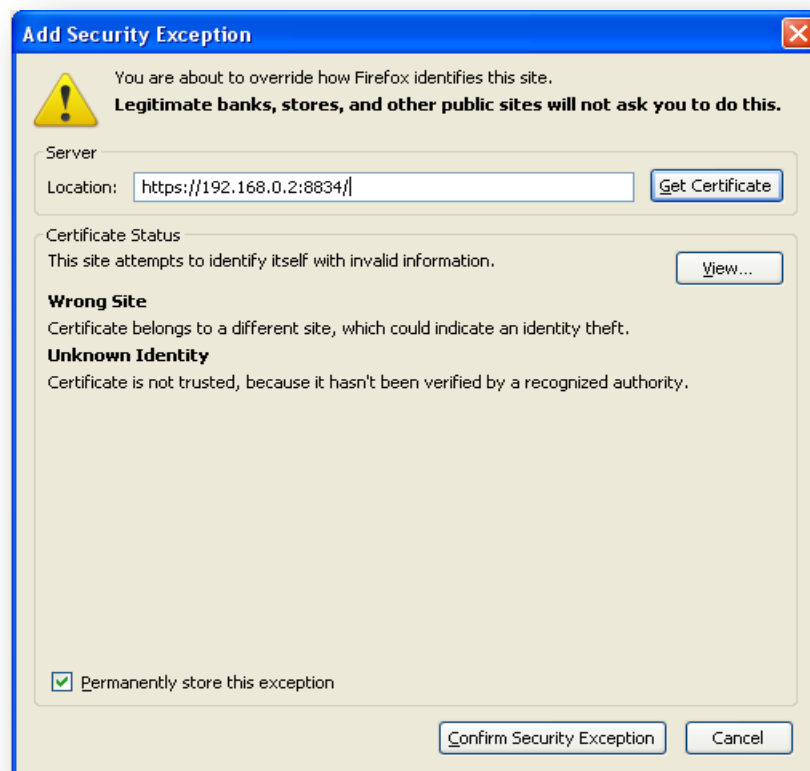
Conexão com a interface do usuário Nessus

Para iniciar a interface do usuário Nessus, proceda da seguinte maneira:

- Abra o navegador de sua preferência.

Digite https://[IP do servidor]:8834/flash.html na barra de navegação.

Certifique-se de se conectar à interface do usuário por meio de HTTPS, pois não são permitidas conexões HTTP sem criptografia.

Ao tentar se conectar à interface do usuário Nessus pela primeira vez, a maioria dos navegadores exibirá um erro indicando que o site não é confiável, devido ao certificado SSL autoassinado:

Os usuários do Microsoft Internet Explorer podem clicar em “Prosseguir para o website (não recomendado)” para carregar a interface do usuário Nessus. Os usuários do Firefox 3.x – 10.x podem clicar em “Eu compreendo os riscos” e, em seguida, em “Adicionar exceção...” para abrir a caixa de diálogo de exceções de sites:

Verifique se a barra “Local:” indica a URL do servidor Nessus e clique em “**Confirm Security Exception**” (Confirmar exceção de segurança). Para obter mais informações sobre como instalar um certificado SSL personalizado, consulte o Guia de Instalação e Configuração do Nessus.

Depois que o navegador confirmar a exceção, a seguinte tela de abertura será exibida:

A tela inicial indicará se o Nessus está registrado com um HomeFeed ou ProfessionalFeed:

Autentique-se usando uma conta e senha criadas com o gerenciador do servidor durante o processo de instalação. Após a autenticação, a interface do usuário exibirá os menus para a criação de políticas, realização de varreduras e pesquisa de relatórios:

Em qualquer ponto durante o uso do Nessus, as opções no canto superior direito estarão presentes. A notação “admin” localizada no canto superior direito da tela acima corresponde à conta conectada no momento. Clique nessa conta para alterar a senha atual. O link “Help” (Ajuda) permite acessar a documentação do Nessus, com instruções detalhadas sobre o uso do software. A opção “About” (Sobre) exibe informações sobre a instalação do Nessus, incluindo versão, tipo de feed, vencimento do feed, versão do cliente e versão do servidor da Web. “Log out” (Sair) encerrará a sessão atual.

Visão geral das políticas

Uma “política” do Nessus consiste em opções de configuração relacionadas à realização de uma varredura de vulnerabilidades. Algumas das opções são, entre outras, as seguintes:

- Parâmetros que controlam aspectos técnicos da varredura, como intervalos de tempo, número de hosts, tipo de scanner de porta etc.
- Credenciais para varreduras locais (por exemplo: Windows, SSH), varreduras autenticadas de bancos de dados Oracle, HTTP, FTP, POP, IMAP ou autenticação pelo Kerberos.
- Especificações individualizadas de varreduras por família ou plugin.
- Verificações de políticas de conformidade de bancos de dados, detalhamento do relatório, definições de varredura de detecção de serviços, verificações de conformidade de Unix, entre outras opções.

Políticas padrão

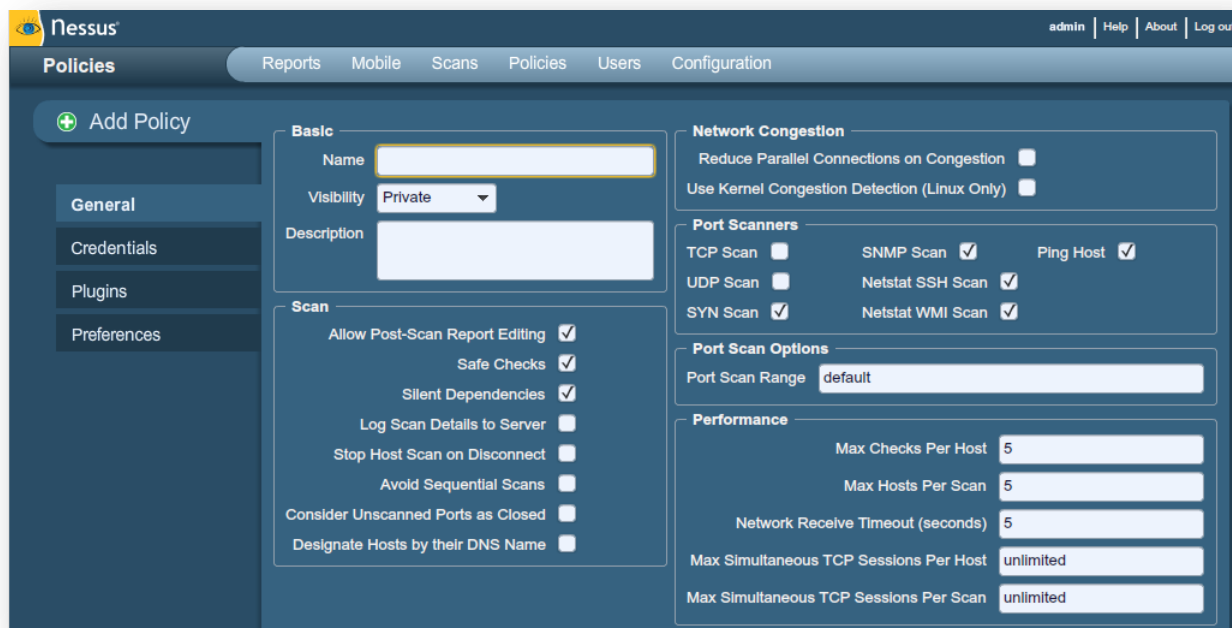
O Nessus é distribuído com várias políticas padrão criadas pela Tenable Network Security, Inc. As políticas são fornecidas como modelos para ajudá-lo a criar políticas adequadas à sua organização ou para serem usadas sem

modificações para varreduras básicas dos seus recursos. Leia e entenda as políticas padrão antes de utilizá-los em varreduras com os seus recursos.

Nome da política	Descrição
Varredura de rede externa	Esta política foi projetada para a verificação de hosts externos e que normalmente apresentam menos serviços à rede. Os plugins relacionados a vulnerabilidades conhecidas de aplicativos da Web (as famílias de plugins CGI Abuses e CGI Abuses: XSS) são ativados com a aplicação desta política. Além disso, todas as 65.536 portas (inclusive a porta 0 por meio de plugin separado) são examinadas em cada destino.
Varredura de rede interna	Esta política foi projetada levando-se em conta a melhoria do desempenho, pois pode ser usada para verificar redes internas de grande porte com muitos hosts, vários serviços expostos e sistemas incorporados, como impressoras. As varreduras de CGI estão desabilitadas e um conjunto de portas padrão é examinado, mas não todas as 65.535.
Testes de aplicativos da Web	Esta política de varredura é usada para verificar os sistemas e fazer com que o Nessus detecte vulnerabilidades conhecidas e desconhecidas nos aplicativos da Web. Os recursos de "difusão" do Nessus são ativados com esta política, o que fará com que o Nessus detecte todos os websites descobertos e verifique as vulnerabilidades presentes em cada um dos parâmetros, incluindo XSS, SQL, injeção de comandos e vários outros. Esta política identificará os problemas via HTTP e HTTPS.
Preparar para auditorias de PCI DSS	Esta política ativa as verificações de conformidade com a norma PCI DSS integradas, compara os resultados das varreduras aos padrões PCI e gera um relatório sobre o comportamento da conformidade. É importante observar que uma varredura de compatibilidade bem-sucedida não garante a conformidade nem uma infraestrutura segura. As organizações que estejam se preparando para uma avaliação da PCI DSS podem usar essa política para preparar suas redes e seus sistemas para a conformidade com a PCI DSS.

Se você pretende usar uma política padrão fornecida pelo Tenable como base para a sua própria política personalizada, use o recurso Copy (Copiar). A edição de uma política padrão fará com que se torne propriedade do usuário e não seja mais exibida na interface.

Como criar uma nova política

Depois de se conectar à interface de usuário do servidor Nessus, é possível criar uma política personalizada ao clicar na opção "**Policies**" (Políticas) na barra superior e no botão **"+ Add**" (Adicionar) à direita. A tela "**Add Policy**" (Adicionar Política) é exibida como no exemplo a seguir:

Observe que existem quatro guias de configuração: **General** (Geral), **Credentials** (Credenciais), **Plugins** e **Preferences** (Preferências). Na maioria dos ambientes, não é necessário modificar as configurações padrão, mas elas permitem um controle mais individualizado sobre o funcionamento do scanner Nessus. Essas guias são descritas a seguir.

General (Geral)

A guia **General** permite nomear a política e configurar as operações de varredura. Há seis caixas de opções agrupadas que controlam o comportamento do scanner:

O painel “**Basic**” (Básico) é usado para definir os aspectos da política em si:

Opção	Descrição
Name (Nome)	Define o nome a ser exibido na interface do usuário Nessus para identificar a política.
Visibility (Visibilidade)	Controla se a política é compartilhada com outros usuários (shared) ou mantida somente para uso privado (private). Somente usuários administrativos podem compartilhar políticas.
Description (Descrição)	Oferece uma breve descrição da política de varredura para resumir a finalidade geral (por exemplo: “varreduras em servidores da Web sem verificações locais ou serviços não HTTP”).

O quadro “**Scan**” (Varredura) define as opções sobre como a varredura deve se comportar:

Opção	Descrição
Allow Post-Scan Report Editing (Permitir a edição do relatório pós-varredura)	Este recurso permite aos usuários excluir itens do relatório quando marcados. Ao fazer uma varredura para conformidade regulatória ou outras auditorias, esta opção deve ser desmarcada para confirmar que a varredura não foi adulterada.

Safe Checks (Verificações Seguras)	A opção Safe Checks (Verificações Seguras) desativa todos os plugins que podem afetar negativamente o host remoto.
Silent Dependencies (Dependências Silencionsas)	Se esta opção for selecionada, a lista de dependências não será incluída no relatório. Se desejar incluir a lista de dependências no relatório, desmarque a caixa de seleção.
Log Scan Details to Server (Salvar detalhes da varredura no log do servidor)	Salva detalhes adicionais da varredura no log do servidor Nessus (`nessusd.messages`), incluindo a ativação ou encerramento do plugin ou se um plugin foi interrompido. O registro resultante pode ser usado para confirmar se determinados plugins foram usados e se os hosts foram examinados.
Stop Host Scan on Disconnect (Cessar a varredura do Host ao desconectar)	Se estiver selecionado, o Nessus cessará a varredura se detectar que o host parou de responder. Isso pode ocorrer se os usuários desligarem seus PCs durante uma varredura, se um host parar de responder depois de um plugin de negação de serviço ou se o mecanismo de segurança (por exemplo: IDS) bloqueou o tráfego para um servidor Se as varreduras continuarem nesses computadores, o tráfego desnecessário será enviado e atrasará a verificação.
Avoid Sequential Scans (Evitar varreduras consecutivas)	Normalmente, o Nessus verifica uma lista de endereços IP em sequência. Se a opção estiver marcada, o Nessus verificará a lista de hosts em ordem aleatória. Isto pode ser útil para ajudar a distribuir o tráfego de rede direcionado a uma sub-rede específica durante varreduras extensas.
Consider Unscanned Ports as Closed (Considerar fechadas as portas não examinadas)	Se uma porta não for examinada com um scanner de porta selecionado (por exemplo: fora do intervalo especificado), será considerada fechada pelo Nessus.
Designate Hosts by their DNS Name (Designar Hosts pelo seu nome DNS)	Deve-se usar o nome do host em vez do endereço IP na impressão do relatório.

O painel “**Network**” (Rede) apresenta opções que controlam melhor a varredura de acordo com a rede de destino a ser verificada:

Opção	Descrição
Reduce Parallel Connections on Congestion (Reduzir conexões paralelas em caso de congestionamento)	Permite que o Nessus detecte o envio de um grande número de pacotes e quando o pipe da rede atingir a capacidade máxima. Se forem detectados, o Nessus reduzirá a velocidade da varredura ao nível adequado para diminuir o congestionamento. Ao diminuir o congestionamento, o Nessus tentará reutilizar o espaço disponível no pipe da rede automaticamente.
Use Kernel Congestion Detection (Linux Only) (Utilizar detecção de congestionamento do Kernel) (Somente Linux)	Permite que o Nessus monitore a CPU e outros mecanismos internos em caso de congestionamento e diminua o ritmo de maneira proporcional. O Nessus tentará usar sempre o máximo de recursos disponível. Este recurso está disponível apenas para os scanners Nessus instalados em Linux.

O painel “**Port Scanners**” (Scanners de Portas) controla os métodos de varredura de portas que devem ser ativados para a varredura:

Opção	Descrição
TCP Scan (Varredura TCP)	Usa o scanner de TCP integrado do Nessus para identificar portas TCP abertas nos alvos. Esse scanner é otimizado e possui alguns recursos de ajuste automático. Em algumas plataformas (por exemplo: Windows e Mac OS X), a seleção do scanner fará com que o Nessus use o scanner SYN para evitar problemas graves de desempenho nativos desses sistemas operacionais.
UDP Scan (Varredura UDP)	Esta opção usa o scanner de UDP integrado do Nessus para identificar as portas UDP abertas nos alvos. O UDP é um protocolo “sem estado”, ou seja, a comunicação não é feita com diálogos de reconhecimento. A comunicação por UDP nem sempre é confiável e, devido à natureza dos serviços UDP e dos dispositivos de rastreamento, nem sempre são detectáveis de maneira remota.
SYN Scan (Varredura SYN)	Usa o scanner de SYN integrado do Nessus para identificar portas TCP abertas nos alvos. As varreduras SYN são um método popular para realizar varreduras de portas e, geralmente, são consideradas um pouco menos invasivas do que as varreduras TCP. O scanner envia um pacote SYN à porta, aguarda a resposta SYN-ACK e determina o estado da porta de acordo com uma resposta ou a falta de resposta.
SNMP Scan (Varredura SNMP)	Instrui o Nessus a examinar alvos para um serviço de SNMP. O Nessus detectará as configurações de SNMP correspondentes durante a varredura. Se as configurações forem feitas pelo usuário em “Preferences” (Preferências), o Nessus examinará totalmente o host remoto e produzirá resultados de auditoria mais detalhados. Por exemplo: muitas verificações do roteador Cisco determinam as vulnerabilidades presentes ao examinar a versão do string SNMP devolvido. Essas informações são necessárias para as auditorias.
Netstat SSH Scan (Varredura SSH Netstat)	Esta opção usa o `netstat` para verificar se há portas abertas no computador local. Depende da disponibilidade do comando `netstat` por meio de uma conexão SSH com o alvo. Esta varredura se destina a sistemas do tipo Unix e requer credenciais de autenticação.
Netstat WMI Scan (Varredura WMI Netstat)	Esta opção usa o `netstat` para verificar se há portas abertas no computador local. Depende da disponibilidade do comando `netstat` por meio de uma conexão WMI com o alvo. Esta varredura se destina a sistemas do tipo Windows e requer credenciais de autenticação. A varredura por WMI usa o `netstat` para determinar portas abertas, portanto, ignora todos os intervalos de portas especificados. Se um enumerador de portas (`Netstat` ou SNMP) for executado, o intervalo de portas torna-se “all” (todas). No entanto, o Nessus manterá a opção “consider unscanned ports as closed” (considerar portas não verificadas como fechadas) se estiver selecionada.

Ping Host (Teste de ping para o Host)	Esta opção permite enviar um teste de "ping" aos hosts remotos em várias portas para determinar se estão "ativos".

O painel **"Port Scan Options"** (Opções de Varredura de Portas) instrui o scanner a localizar um intervalo de portas específico. Os valores a seguir são permitidos para a opção "Port Scan Range" (Intervalo de varredura de portas):

Valor	Descrição
"default" (Predefinidas)	Se a palavra-chave "default" (predefinidas) for usada, o Nessus examinará cerca de 4.790 portas comuns. A lista de portas pode ser encontrada no arquivo `nessus-services`.
"all" (todas)	Se a palavra-chave "all" for usada, o Nessus examinará todas as 65.535 portas.
Custom List (Lista personalizada)	Um intervalo personalizado de portas pode ser selecionado com o uso de uma lista delimitada por vírgulas de portas ou intervalos de portas. Por exemplo: é possível usar "21,23,25,80,110" ou "1-1024,8080,9000-9200". A opção "1-65535" verificará todas as portas. Pode-se especificar também um intervalo de divisão específico para cada protocolo. Por exemplo: para verificar um intervalo de portas diferente para TCP e UDP na mesma política, é preciso especificar "T:1-1024,U:300-500". Pode-se especificar também um conjunto de portas para varredura em ambos os protocolos, bem como intervalos individuais para cada protocolo separado ("1-1024,T:1024-65535,U:1025"). Se um único protocolo for verificado, selecione somente o scanner para aquela porta e especifique as portas normalmente.

O intervalo especificado para uma varredura de portas será aplicado às varreduras TCP e UDP.

O painel "**Performance**" (Desempenho) possui duas opções que controlam o número de varreduras a ser iniciado. Essas opções podem ser as mais importantes ao configurar uma varredura, pois têm maior impacto sobre o tempo de varredura e a atividade da rede.

Opção	Descrição
Max Checks Per Host (Máx. verificações por Host)	Esta configuração limita o número máximo de verificações que um scanner Nessus realiza em um único host ao mesmo tempo.
Max Hosts Per Scan (Máx. Hosts varredura)	Esta configuração limita o número máximo de hosts que um scanner Nessus pode verificar ao mesmo tempo.
Network Receive Timeout (seconds) (Tempo de espera por resposta da rede) (segundos)	O valor padrão é cinco segundos. Esse é o tempo que o Nessus deve esperar por uma resposta do host, exceto se definido com outro valor por um plugin. Se a varredura for feita em uma conexão lenta, será preciso definir este valor com um número maior de segundos.
Max Simultaneous TCP Sessions Per Host (Máx. sessões TCP	Esta configuração limita o número máximo de sessões TCP estabelecidas para um único host.

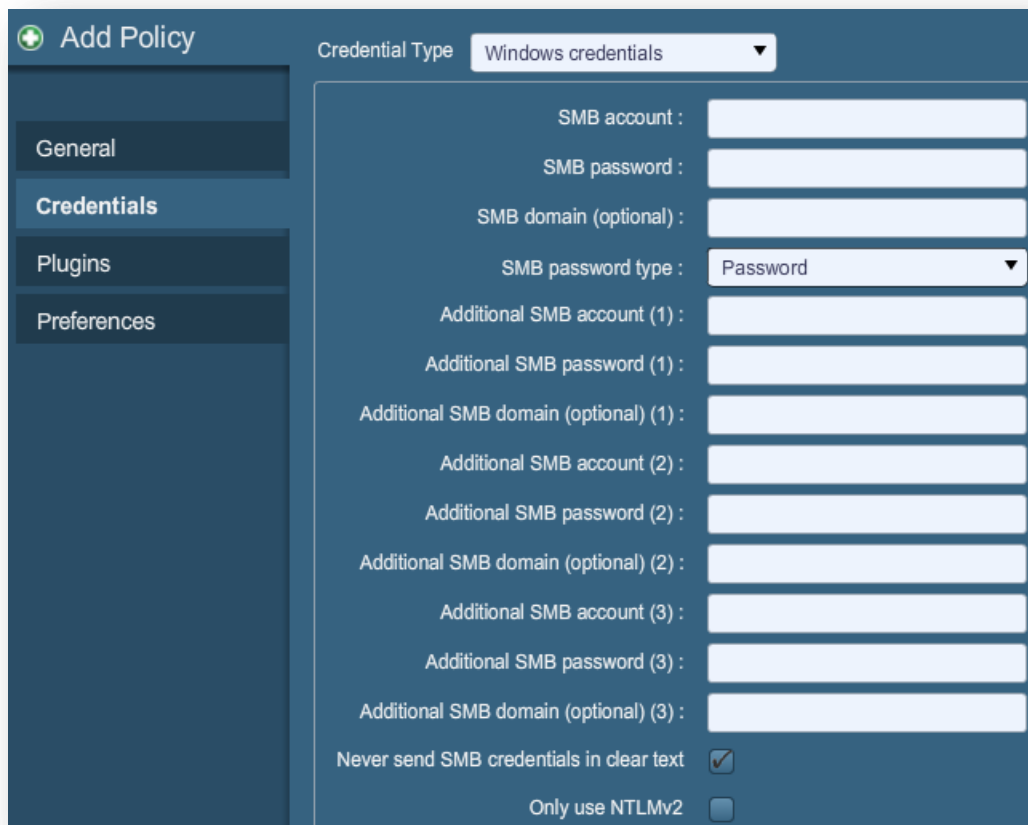
simultâneas para um Host)	Esta opção de congestionamento de TCP também controla o número de pacotes por segundo que o scanner SYN enviará (por exemplo: se esta opção estiver definida como 15, o scanner SYN enviará 1.500 pacotes por segundo, no máximo).
Max Simultaneous TCP Sessions Per Scan (Máx. sessões TCP simultâneas para uma varredura)	Esta configuração limita o número máximo de sessões TCP estabelecidas para toda a varredura, independentemente do número de hosts verificados. Para os scanners Nessus instalados em computadores com Windows XP, Vista e 7, este valor deve ser de no máximo 19 para se obter resultados precisos.

Credentials (Credenciais)

A guia **Credentials** (Credenciais) na imagem abaixo permite configurar o scanner Nessus para o uso de credenciais de autenticação durante a varredura. A definição de credenciais permite que o Nessus realize um número maior de verificações e gere resultados de varredura mais precisos.

O item de menu suspenso "**Windows credentials**" (Credenciais do Windows) possui configurações para fornecer ao Nessus informações, como o nome da conta SMB, senha e nome do domínio. O protocolo SMB (bloqueio de mensagens do servidor) é um protocolo de compartilhamento de arquivos que permite aos computadores compartilhar informações de forma transparente através da rede. Se as informações forem fornecidas, o Nessus poderá encontrar informações locais de um host Windows remoto. Por exemplo: o uso de credenciais permite que o Nessus determine se foram aplicados patches de segurança importantes. Não é necessário modificar outros parâmetros de SMB em relação às configurações padrão.

Quando diversas contas SMB forem configuradas, o Nessus tentará fazer o login com as credenciais fornecidas em sequência. Depois de ser autenticado com um conjunto de credenciais, o Nessus irá verificar as credenciais fornecidas subsequentes, mas só irá usá-las se os privilégios administrativos forem concedidos com o acesso do usuário pré-fornecido com as contas.

Algumas versões do Windows permitem criar uma nova conta e designá-la como um "administrator". Essas contas nem sempre são adequadas para fazer varreduras com credenciais. A Tenable recomenda que a conta administrativa original, denominada "Administrator", seja usada para varreduras com credenciais, para garantir que o acesso integral seja permitido. Em algumas versões do Windows, essa conta pode estar oculta. A conta de administrador real pode ser reexibida executando um prompt do DOS com privilégios administrativos e digitando o seguinte comando:

```
C:\> net user administrator /active:yes
```

Se uma conta SMB de manutenção for criada com privilégios limitados de administrador, o Nessus poderá realizar varreduras em diversos domínios de maneira fácil e segura.

A Tenable recomenda que os administradores de rede criem contas específicas de domínio para facilitar os testes. O Nessus conta com diversas verificações de segurança para Windows NT, 2000, Server 2003, XP, Vista, Windows 7 e Windows 2008, que serão mais precisas se uma conta de domínio for fornecida. Na maioria dos casos, o Nessus tentará aplicar diversas verificações caso uma conta não seja fornecida.

O serviço de registro remoto do Windows permite que computadores remotos com credenciais acessem o registro do computador a ser auditado. Se o serviço não estiver em execução, não será possível ler chaves e valores do registro, mesmo com credenciais completas. Para obter mais informações, consulte o artigo "Dynamic Remote Registry Auditing - Now you see it, now you don't!" no blog da Tenable. Esse serviço deve ser iniciado para que uma varredura com credenciais do Nessus audite integralmente um sistema usando credenciais.

Os usuários podem selecionar "**SSH settings**" (Configurações SSH) no menu suspenso e inserir credenciais para a varredura de sistemas Unix. As credenciais são usadas para obter informações locais de sistemas Unix remotos para auditoria de patches ou verificações de conformidade. Existe um campo para a inserção do nome de usuário do SSH da conta que realizará as verificações no sistema Unix de destino, juntamente com a senha ou chave pública do SSH e um par de chaves privadas. Existe também um campo para a inserção da frase-senha da chave SSH, se necessário.

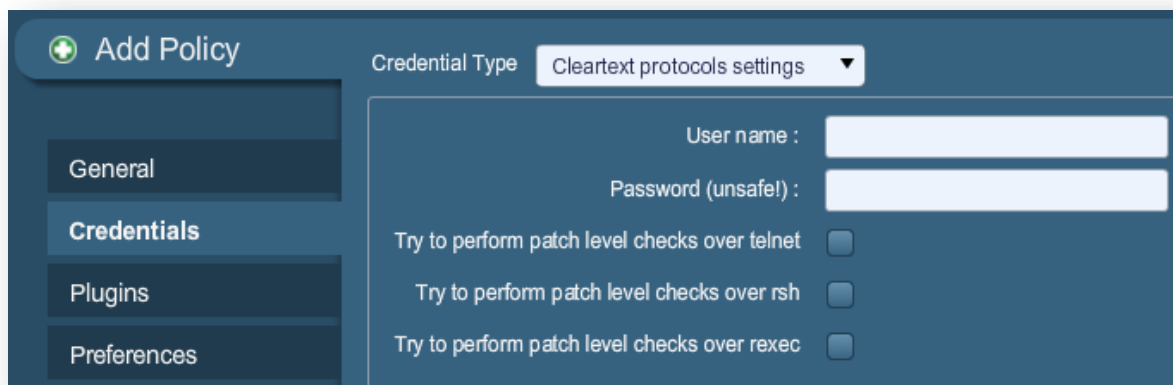
O Nessus 4 permite o uso dos algoritmos criptográficos **`blowfish-cbc`**, **`aes-cbc`** e **`aes-ctr`**.

As varreduras credenciadas mais eficazes são aquelas em que as credenciais fornecidas têm privilégios "root". Uma vez que muitos locais não permitem o login remoto como root, os usuários do Nessus podem acessar "**`su`**", "**`sudo`**", "**`su+sudo`**" ou "**`dzdo`**" com uma senha distinta em uma conta criada para ter os privilégios "**`su`**" ou "**`sudo`**". Além disso, o Nessus pode atribuir privilégios em dispositivos Cisco ao selecionar "**`Cisco 'enable'`**".

O Nessus pode usar o acesso por chaves SSH para se autenticar em um servidor remoto. Se um arquivo SSH **`known_hosts`** estiver disponível e fornecido com base na política de varredura, o Nessus tentará fazer o login apenas nos hosts deste arquivo. Além disso, a opção "Preferred SSH port" (Porta SSH preferencial) pode ser configurada para indicar ao Nessus que se conecte com o SSH se estiver funcionando em uma porta que não seja a porta 22.

O Nessus criptografa todas as senhas armazenadas nas políticas. No entanto, as boas práticas recomendam o uso de chaves SSH (e não senhas SSH) para autenticação. Isso ajuda a assegurar que o mesmo nome de usuário e senha usados para auditar os servidores SSH conhecidos não sejam usados para efetuar o login em um sistema que não esteja sob seu controle. Dessa forma, não é recomendável usar senhas SSH, a menos que seja absolutamente necessário.

O Nessus também oferece uma opção “su+sudo”, que pode ser usada caso um sistema não conceda privilégios de login remotos a contas privilegiadas.

A captura de tela a seguir mostra as opções SSH disponíveis. O menu suspenso “Elevate privileges with” (Elevar privilégios com) fornece os vários métodos de elevar os privilégios após serem autenticados.

Se outra conta for usada além de `root` para elevação de privilégios, pode ser especificada em “**Escalation account**” (Elevação de conta) com a opção “**Escalation password**” (Senha de elevação).

“**Kerberos configuration**” (Configuração do Kerberos) permite especificar credenciais com o uso de chaves do Kerberos a partir de um sistema remoto:

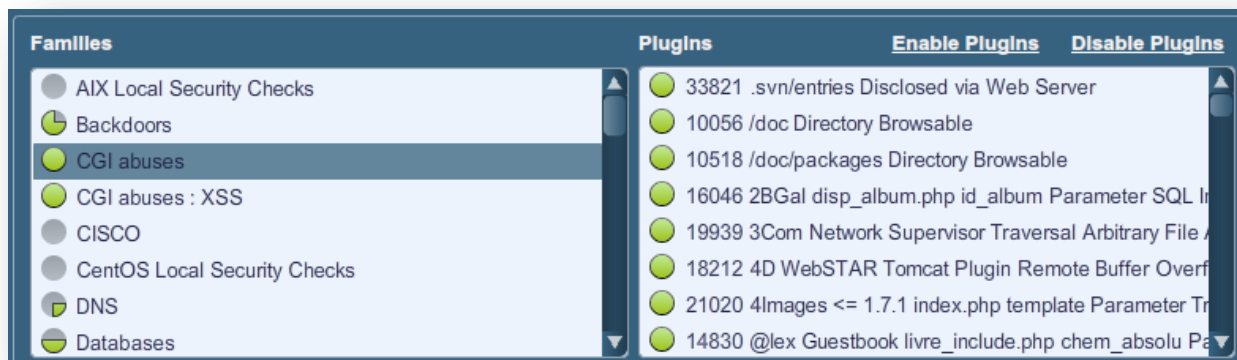
Além disso, se um método seguro de varreduras credenciadas não estiver disponível, os usuários podem forçar o Nessus a executar varreduras por meio de protocolos sem segurança ao selecionar o item “**Cleartext protocol settings**” (Configurações de protocolo de texto simples) no menu suspenso. Os protocolos de texto simples disponíveis para esta opção são **telnet**, **rsh** e **rexec**.

Normalmente, todas as senhas (e a própria política) são criptografadas. Se a política for salva em um arquivo `.nessus` e o arquivo `.nessus` for posteriormente copiado em uma instalação do Nessus distinta, nenhuma senha da política poderá ser usada pelo segundo scanner Nessus, pois não será capaz de decodificá-las.

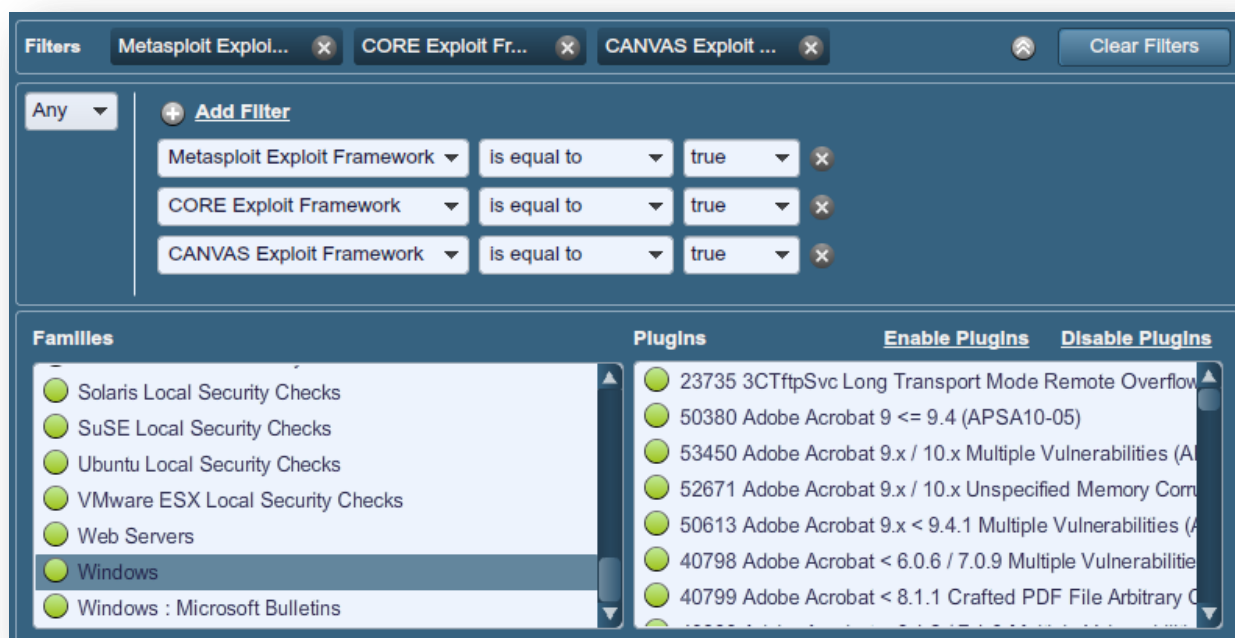
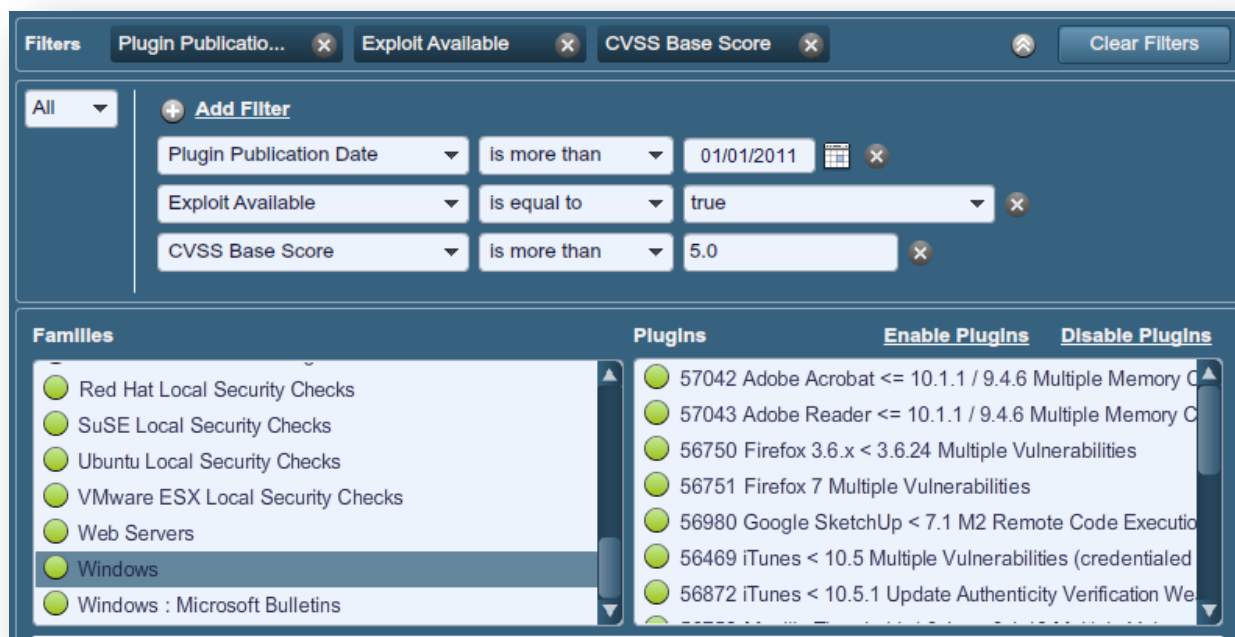
Não é recomendável usar credenciais em texto simples de qualquer tipo. Se as credenciais forem enviadas de maneira remota (por meio de uma varredura do Nessus, por exemplo), elas poderão ser interceptadas por qualquer pessoa com acesso à rede. Use mecanismos de autenticação criptografada sempre que possível.

Plugins

A guia **Plugin** permite que o usuário escolha verificações de segurança específicas por família de plugin ou verificações individuais.

É possível clicar no círculo amarelo ao lado de uma família de plugins para ativar (verde) ou desativar (cinza) a família inteira. A seleção da família exibirá a lista dos plugins no painel superior direito. Plugins individuais podem ser ativados ou desativado para criar políticas de varredura específicas. Depois que os ajustes forem feitos, o número total de famílias e plugins selecionados será exibido na parte inferior. Se o círculo ao lado de uma família de plugins ficar 25%, 50% ou 75% verde, isso indica que alguns plugins estão ativados, mas nem todos eles.

A seleção de um plugin específico mostrará o resultado do plugin a ser exibido como em um relatório. O resumo e a descrição fornecerão mais detalhes sobre a vulnerabilidade a ser examinada. Ao rolar o painel "Plugin Description" (Descrição dos plugins) para baixo, é possível ver mais referências, se estiverem disponíveis, e a pontuação CVSSv2, que apresenta uma classificação básica de risco.

Na parte superior da guia da família de plugins, é possível criar filtros para construir uma lista de plugins a serem incluídos na política. Os filtros permitem o controle granular sobre a seleção de plugins. Vários filtros podem ser definidos em uma única política. Para criar um filtro, clique no link “**Add Filter**” (Adicionar filtro):

Cada filtro criado oferece várias opções para refinar a busca. Os critérios de filtragem podem se basear em “Any” (Qualquer), em que qualquer critério retornará coincidências, ou “All” (Todos), em que todos os critérios de filtragem devem estar presentes. Por exemplo: para pesquisar uma política que inclui apenas plugins que têm um exploit associado em um quadro de exploit comercial, é possível criar três filtros e selecionar “Any” (Qualquer) como critério:

Para criar uma política que contenha plugins que correspondam a vários critérios, é possível selecionar “All” (Todos) e adicionar os filtros desejados. Por exemplo: a política a seguir deve incluir qualquer plugin publicado após 1 de Janeiro de 2011 com um exploit público e CVSS Base Score (Pontuação CVSS base) superior a 5.0:

Para obter uma lista completa de critérios de filtragem, consulte a seção Filtros de relatórios deste documento.

Para usar filtros para a criação de políticas, recomenda-se começar desativando todos os plugins. Usando os filtros de plugins, selecione apenas os plugins que deseja incluir na política. Depois de concluído, selecione cada família de plugins e clique em “Enable Plugins”.(Ativar plugins).

Ao criar e salvar uma política, todos os plugins selecionados inicialmente são armazenados. Quando novos plugins forem recebidos com a atualização de feeds de plugins, serão ativados automaticamente se a família à qual estiverem associados for ativada. Se a família estiver desativada ou parcialmente ativada, os novos plugins da família também serão desativados automaticamente.

A família “Denial of Service” (Negação de serviço) contém alguns plugins que podem causar falhas em uma rede corporativa caso a opção “Safe Checks” (Verificações Seguras) não estiver ativa, mas contém algumas verificações úteis que não causam danos. A família “Denial of Service” (Negação de serviço) pode ser usada junto com “Safe Checks” (Verificações Seguras) para garantir que nenhum plugin potencialmente nocivo seja executado. No entanto, recomenda-se que a família “Denial of Service” (Negação de serviço) não seja usada em uma rede de produção.

Abaixo da janela que mostra os plugins, o usuário encontrará duas opções que o ajudarão a selecionar e visualizar os plugins.

Opção	Descrição
Show Only Enabled Plugins (Mostrar somente Plugins ativos)	A seleção desta opção fará com que o Nessus mostre apenas os plugins selecionados manualmente ou por meio de filtro.
Enable all (Ativar todos)	Verifica e ativa todos os plugins e suas famílias. É a maneira conveniente de reativar todos os plugins depois de criar uma política com algumas famílias ou plugins desativados. Observe que alguns plugins podem exigir opções de configuração adicionais.
Disable all (Desativar todos)	Desmarca e desativa todos os plugins e suas famílias. A execução de uma varredura com todos os plugins desativados não irá gerar nenhum resultado.

Preferences (Preferências)

A guia “**Preferences**” (Preferências) contém meios de controle individualizados para configuração de varreduras. Selecione um item no menu suspenso para exibir itens de configuração adicionais para a categoria selecionada. Observe que esta é uma lista dinâmica de opções de configuração e depende do feed de plugins, das políticas de auditoria e de outras funções às quais o scanner Nessus conectado tem acesso. Um scanner com ProfessionalFeed pode ter opções de configuração mais avançadas do que um scanner configurado com o HomeFeed. Esta lista também pode mudar à medida que os plugins são adicionados ou modificados.

A tabela a seguir oferece uma descrição geral de todas as preferências. Para obter informações detalhadas com relação a cada item de preferência, consulte a seção Verificação de preferências detalhadas neste documento.

Menu Preference (Preferências)	Descrição
ADSI settings (Configurações de ADSI)	O Active Directory Service Interfaces obtém informações do servidor MDM (Mobile Device Management) sobre dispositivos Android e iOS.
Apple Profile Manager API Settings (Configurações de API Apple Profile Manager)	Um recurso do ProfessionalFeed que habilita enumeração e varredura de vulnerabilidades para dispositivos com Apple iOS (por exemplo, iPhone, iPad).

Cisco IOS Compliance Checks (Verificações de conformidade de Cisco IOS)	Opção de ProfessionalFeed que permite que um arquivo de política seja especificado para testar dispositivos Cisco IOS com base em padrões de conformidade.
Database Compliance Checks (Verificações de conformidade de banco de dados)	Opção de ProfessionalFeed que permite que um arquivo de política seja especificado para testar bancos de dados DB2, SQL Server, MySQL e Oracle com base em padrões de conformidade.
Database Settings (Configurações de banco de dados)	Opções usadas para especificar o tipo de banco de dados a ser verificado, bem como as credenciais a serem usadas.
Do not scan fragile devices (Não verificar dispositivos frágeis)	Conjunto de opções que instrui o Nessus a **não** verificar dispositivos específicos devido ao risco de danificar o alvo.
Global variable settings (Configurações globais de variáveis)	Grande variedade de opções de configuração para o Nessus.
HTTP cookies import (Importação de cookies HTTP)	Para os testes de aplicativos da web, esta preferência especifica um arquivo externo para a importação de cookies HTTP, de modo a permitir a autenticação do aplicativo.
HTTP login page (Página de login HTTP)	Definições relacionadas à página de login para testes de aplicativos da Web.
IBM iSeries Compliance Checks (Verificações de conformidade IBM iSeries)	Opção de ProfessionalFeed que permite que um arquivo de política seja especificado para teste de sistemas IBM iSeries com base em padrões de conformidade.
IBM iSeries Credentials (Credenciais para IBM iSeries)	Opção que especifica as credenciais para sistemas IBM iSeries.
ICCP/COTP TSAP Addressing Weakness (Atenção de fraquezas ICCP/COTP TSAP)	Uma opção ProfessionalFeed relacionada aos testes Controle de supervisão e aquisição de dados (SCADA).
Login configurations (Configurações de Login)	Local em que as credenciais são especificadas para teste de serviços HTTP, NNTP, FTP, POP e IMAP básicos.
Modbus/TCP Coil Access (Acesso Modbus/TCP Coil)	Uma opção ProfessionalFeed relacionada aos testes Controle de supervisão e aquisição de dados (SCADA).
Nessus SYN scanner (Scanner Nessus SYN)	Opções relacionadas ao scanner SYN integrado.
Nessus TCP scanner (Scanner Nessus TCP)	Opções relacionadas ao scanner TCP integrado.
News Server (NNTP) Information Disclosure (Divulgação de informações nos servidores de notícias (NNTP))	Um conjunto de opções que verifica a presença de vulnerabilidades de divulgação de informações nos servidores NNTP.
Oracle Settings (Configurações de Oracle)	Opções relacionadas às instalações de banco de dados do Oracle.
PCI DSS compliance (Conformidade PCI DSS)	Opção do ProfessionalFeed que instrui o Nessus a comparar os resultados de varredura com relação aos PCI DSS standards.
Patch Management: Red Hat Satellite Server Settings	Opções de integração do Nessus com o servidor de gerenciamento de patches Red Hat Satellite. Consulte o documento Patch Management

(Gerenciamento de patches: Configurações do servidor Red Hat Satellite)	Integration para obter mais informações.
Patch Management: SCCM Server Settings (Gerenciamento de patches: Configurações do servidor SCCM)	Opções de integração do Nessus com o servidor de gerenciamento de patches System Center Configuration Manager (SCCM). Consulte o documento Patch Management Integration para obter mais informações.
Patch Management: VMware Go Server Settings (Gerenciamento de patches: Configurações do servidor VMware Go)	Opções de integração do Nessus com o servidor de gerenciamento de patches VMware Go Server (Shavlik). Consulte o documento Patch Management Integration para obter mais informações.
Patch Management: WSUS Server Settings (Gerenciamento de patches: Configurações do servidor WSUS)	Opções de integração do Nessus com o servidor de gerenciamento de patches Windows Server Update Service (WSUS) (Serviço de atualizaçao do Servidor Windows). Consulte o documento Patch Management Integration para obter mais informações.
Ping the remote host (Ping do Host remoto)	Opções que permitem controlar descobertas de rede com base no ping do Nessus.
Port scanner settings (Configurações de varredura de portas)	Duas opções que oferecem mais controle sobre a atividade de varredura de portas.
SMB Registry: Start the Registry Service during the scan (Registro SMB: Iniciar o serviço de registro durante a varredura)	Instrui o Nessus a iniciar o serviço de registro SMB em hosts que não o possuem ativado.
SMB Scope (Alcance do SMB)	Instrui o Nessus a consultar os usuários do domínio em vez dos usuários locais.
SMB Use Domain SID to Enumerate Users (SMB usar domínio SID para enumerar usuários)	Opção que permite especificar o intervalo de SID para pesquisas SMB de usuários do domínio.
SMB Use Host SID to Enumerate Local Users (SMB usar Host SID para enumerar usuários locais)	Opção que permite especificar o intervalo de SID para pesquisas SMB de usuários locais.
SMTP Settings (Configurações de SMTP)	Opções de verificação de Simple Mail Transport Protocol (SMTP).
SNMP Settings (Configurações de SNMP)	Informações de configuração e autenticação para Simple Network Management Protocol (SNMP).
Service Detection (Detecção do serviço)	Opções que permitem ao Nessus verificar os serviços baseados em SSL.
Unix Compliance Checks (Verificações de conformidade Unix)	Opção de ProfessionalFeed que permite que um arquivo de política seja especificado para teste de sistemas Unix com base em padrões de conformidade.
VMware SOAP API Settings (Configurações de VMware SOAP API)	Informações de configuração e autenticação para SOAP APIs da VMware.

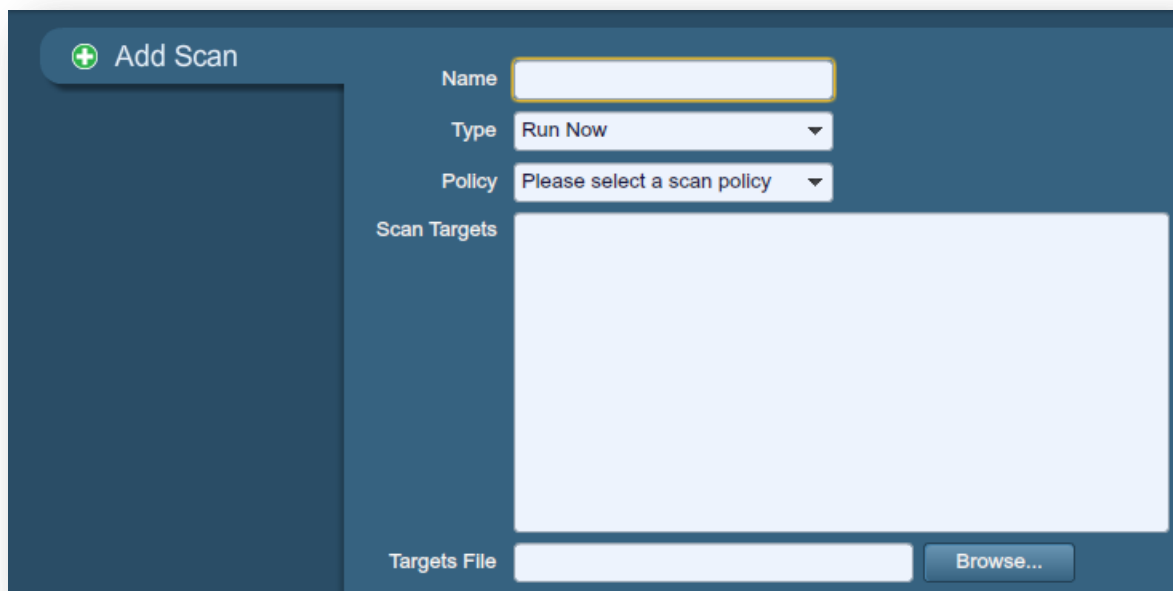
Wake-on-LAN (Arranque remoto de LAN)	Instrui o Nessus a enviar pacotes Wake-on-LAN (WOL) antes de executar uma varredura.
Web Application Test Settings (Configurações de testes de aplicativos da Web)	Opções relacionadas a testes de aplicativos da Web.
Web mirroring (Espelhamento da Web)	Detalhes de configuração que controlam o número de páginas da Web que o Nessus irá espelhar para analisar o conteúdo das vulnerabilidades.
Windows Compliance Checks (Verificações de conformidade Windows)	Opção de ProfessionalFeed que permite que um arquivo de política seja especificado para teste de sistemas Windows com base em padrões de conformidade.
Windows File Contents Compliance Checks (Verificações de conformidade do conteúdo de arquivos Windows)	Opção de ProfessionalFeed que permite que um arquivo de política seja especificado para teste de arquivos do sistema Windows com base em padrões de conformidade.

Devido às atualizações de metadados do XML no Nessus 5, os dados de conformidade gerados com o Nessus 4 não estarão disponíveis no capítulo de verificações de conformidade dos relatórios exportados. No entanto, os dados de conformidade estarão disponíveis na interface do usuário Nessus via Web.

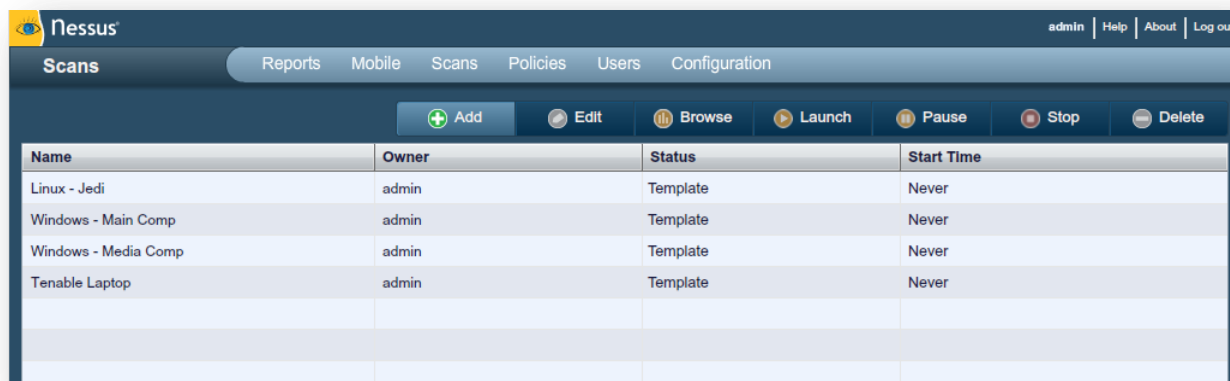
Importar, exportar e copiar políticas

O botão “**Import**” (Importar) no canto superior esquerdo permite enviar políticas criadas ao scanner. Na caixa de diálogo “**Browse**” (Procurar...), selecione a política no sistema local e clique em “**Submit**” (Enviar).

O botão “**Export**” (Exportar) na barra de menus permite baixar uma política existente do scanner para o sistema de arquivos local. A caixa de diálogo de download do navegador permite abrir a política em um programa externo (por exemplo: editor de texto) ou salvá-la em um diretório de sua preferência.

As senhas e os arquivos .audit presentes em uma política **não** serão exportados.

Para criar uma política semelhante à uma política existente, mas com algumas modificações, selecione a política básica na lista e clique em “**Copy**” (Copiar) na barra de menus superior direita. Isso criará uma cópia da política original, que

pode ser editada com as modificações necessárias. Isso permite criar políticas padrão com algumas alterações necessárias para um determinado ambiente.

Criar, iniciar e programar uma varredura

Depois de criar uma política, é possível criar uma nova varredura ao clicar na opção “**Scans**” (Varreduras) na barra de menus superior e no botão “**+ Add**” (Adicionar) à direita. A tela “**Add Scan**” (Adicionar Varredura) será exibida da seguinte maneira:

Existem cinco campos para informar o alvo da varredura:

- **Name** (Nome) – Define o nome que será exibido na interface do usuário do Nessus para identificar a política.
- **Type** (Tipo) – Selecione “Run Now” (executar imediatamente a varredura após o envio), “Scheduled” (horário em que a varredura deve começar) ou “Template” (salvar como modelo para varreduras recorrentes).
- **Policy** (Política) – Selecione uma política já criada a ser usada pela varredura para definir os parâmetros que controlam o comportamento de varredura do servidor Nessus.

- **Scan Targets** (Alvos da varredura) – Os alvos podem ser inseridos com um endereço IP simples (por exemplo: 192.168.0.1), um intervalo de IPs (por exemplo: 192.168.0.1-192.168.0.255), uma sub-rede com a notação CIDR (por exemplo: 192.168.0.0/24) ou um host conversível (por exemplo: www.nessus.org).

- **Targets File** (Arquivo de alvos) – É possível importar um arquivo de texto com uma lista de hosts ao clicar em "**Browse…**" (Procurar) e selecionar um arquivo no computador local.

O arquivo de host deve ser formatado como texto ASCII, com um host por linha e sem espaços ou linhas extras. A codificação Unicode/UTF-8 não é reconhecida.

Exemplo de formatos de arquivos de host:

Hosts individuais:

192.168.0.100
192.168.0.101
192.168.0.102

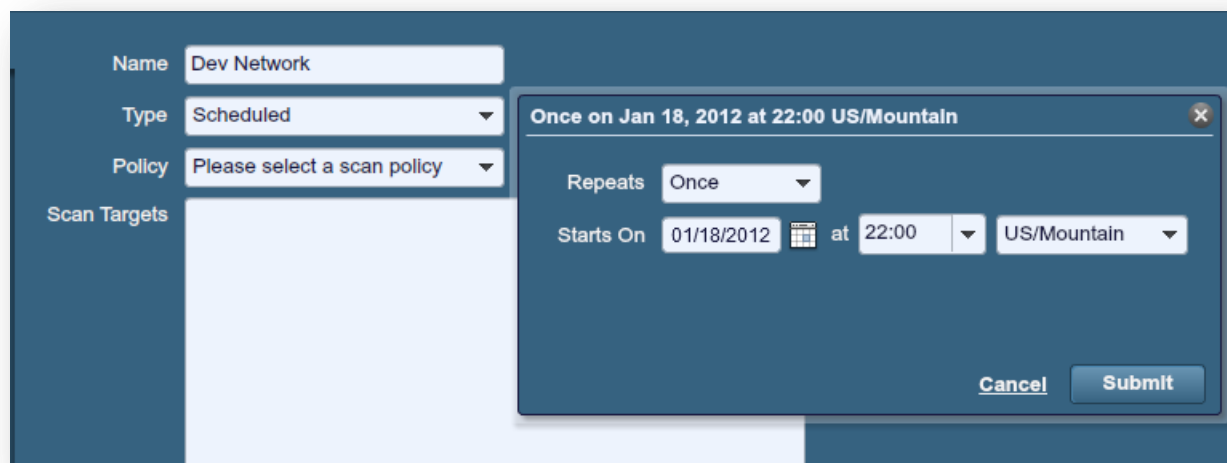
Intervalo de hosts:

192.168.0.100-192.168.0.102

Bloco CIDR de hosts:

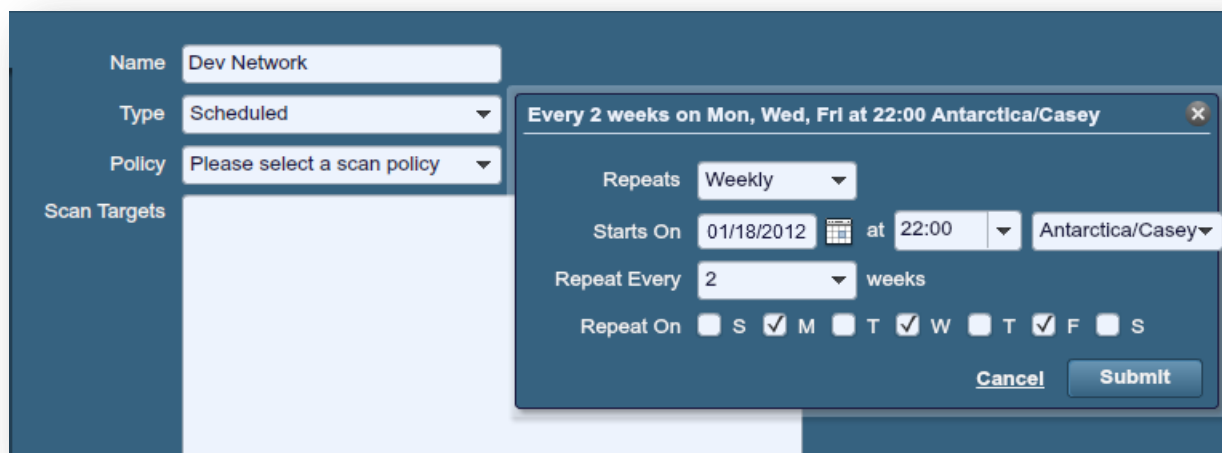
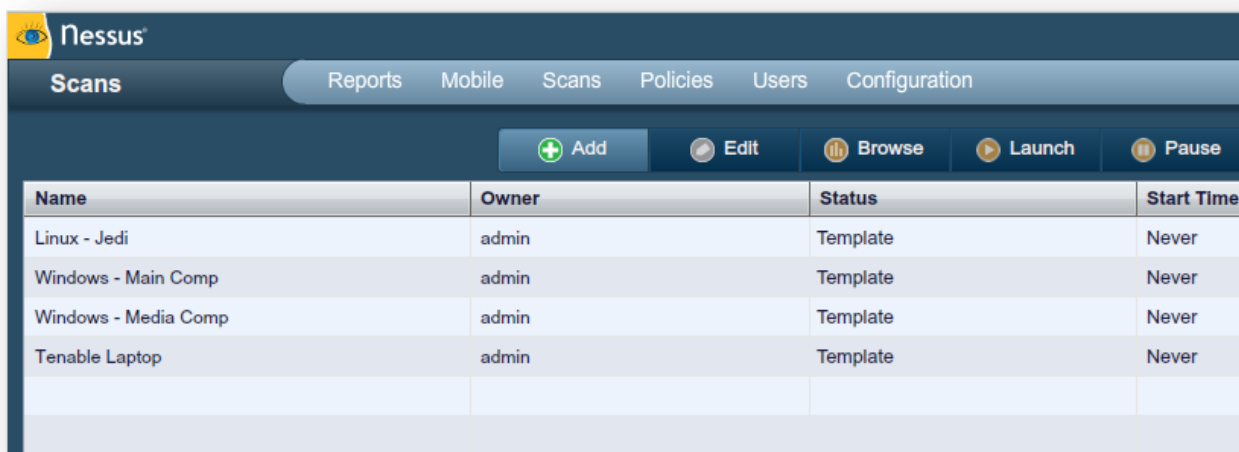
192.168.0.1/24

Servidores virtuais:

www.tenable.com[192.168.1.1]
www.nessus.org[192.168.1.1]
www.tenablesecurity.com[192.168.1.1]

Depois de inserir as informações de varredura, clique em "**Submit**" (Enviar). Depois do envio, a varredura iniciará imediatamente (se "Run Now" for selecionado) antes que a tela retorne à página geral de "**Scans**" (Varreduras).

Depois que a varredura for iniciada, a lista Scans exibirá todas as varreduras em execução, em pausa ou em forma de modelo, além de informações básicas sobre cada varredura. Depois de selecionar uma varredura específica na lista, os botões de ação no canto superior direito permitem **"Pesquisar"** os resultados da varredura em progresso, **"Pausar"** e **"Reiniciar"** a varredura ou **"Parar"** e **"Excluir"** totalmente a varredura. Os usuários podem também **"Editar"** os modelos de varreduras.

Quando for concluída por qualquer motivo, a varredura será retirada da lista “**Scans**” (varreduras) e estará disponível para revisão na guia “**Reports**” (Relatórios).

Se uma varredura estiver designada como “Scheduled” (Programada), uma opção será exibida para definir o horário de início desejado e a frequência:

No menu suspenso “Repeats” (Repetições), a varredura pode ser programada para ser executada uma única vez, diariamente, semanalmente, mensalmente ou anualmente. Essa opção também pode ser especificada para iniciar em uma data e horário específicos. Após salvar a varredura, o Nessus iniciará a varredura no horário especificado.

As varreduras programadas estão disponíveis apenas para os clientes do ProfessionalFeed.

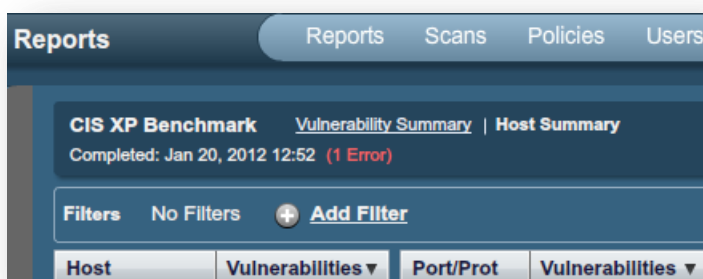
Se uma varredura for salva como um modelo, aparecerá na lista de varreduras dessa maneira e aguardará para ser iniciada.

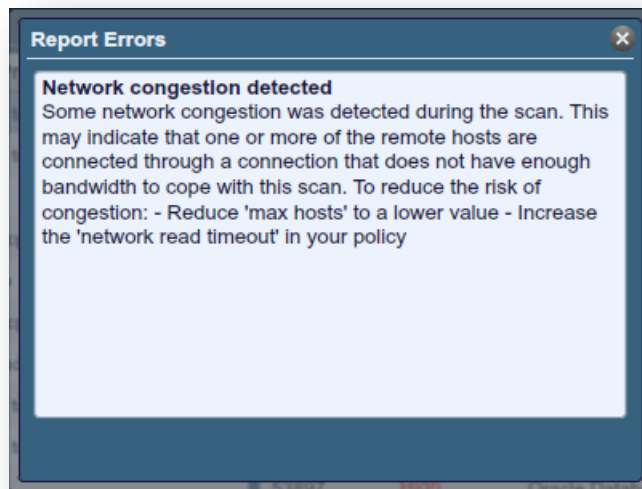
Relatórios

Com o lançamento do Nessus 5, os usuários podem criar seu próprio relatório por capítulos: Vulnerability Centric, Host Centric, Compliance ou Compliance Executive. O formato HTML ainda é o padrão. No entanto, se o Java estiver instalado no host do scanner, também é possível exportar relatórios em PDF. Com o uso de filtros de relatório e os recursos de exportação, os usuários podem criar relatórios dinâmicos à sua própria escolha em vez de selecioná-los em uma lista específica.

Ao clicar no guia "**Reports**" (Relatórios) na barra de menus superior da interface, a lista de varreduras em execução e concluídas será exibida:

A tela "**Reports**" (Relatórios) funciona como um ponto central para exibir, comparar, enviar e baixar resultados de varreduras. Use a tecla "Shift" ou "Ctrl" para selecionar vários relatórios de uma só vez.

Browse (Procurar)

Para pesquisar os resultados de uma varredura, selecione um nome na lista “**Reports**” (Relatórios) e clique em “**Browse**” (Procurar). Isso permite exibir os resultados ao navegar pelas vulnerabilidades ou hosts, exibir portas e informações de vulnerabilidades específicas. A exibição padrão é feita por resumo de vulnerabilidades, que mostra cada vulnerabilidade encontrada classificada por gravidade:

Se ocorrer algum erro durante a varredura, haverá uma notação próxima à data “Completed”. Clique no erro para fornecer mais informações:

Na exibição “**Vulnerability Summary**” (Resumo de vulnerabilidades), o usuário pode remover vulnerabilidades do relatório de maneira seletiva. Ao selecionar uma vulnerabilidade, informações adicionais, como o(s) host(s) e porta(s) afetado(s) serão exibidas, juntamente com detalhes técnicos da vulnerabilidade. No canto superior direito, “**Remove Vulnerability**” (Remover vulnerabilidade) pode ser usada para excluir a vulnerabilidade selecionada:

À medida que o usuário navega pelos resultados de varredura, a interface do usuário exibe uma lista de hosts e portas afetados, bem como informações adicionais sobre a vulnerabilidade:

Para alternar entre as exibições de resumo de vulnerabilidades e resumo de hosts, selecione a exibição desejada na parte superior da tela ao lado do nome da varredura:

Selecione um host para exibir todos os resultados de vulnerabilidade associados ao host por porta:

Lab Network /24 | Vulnerability Summary | Host Summary | Download Report
Completed: Jan 18, 2012 22:27 | Audit Trail

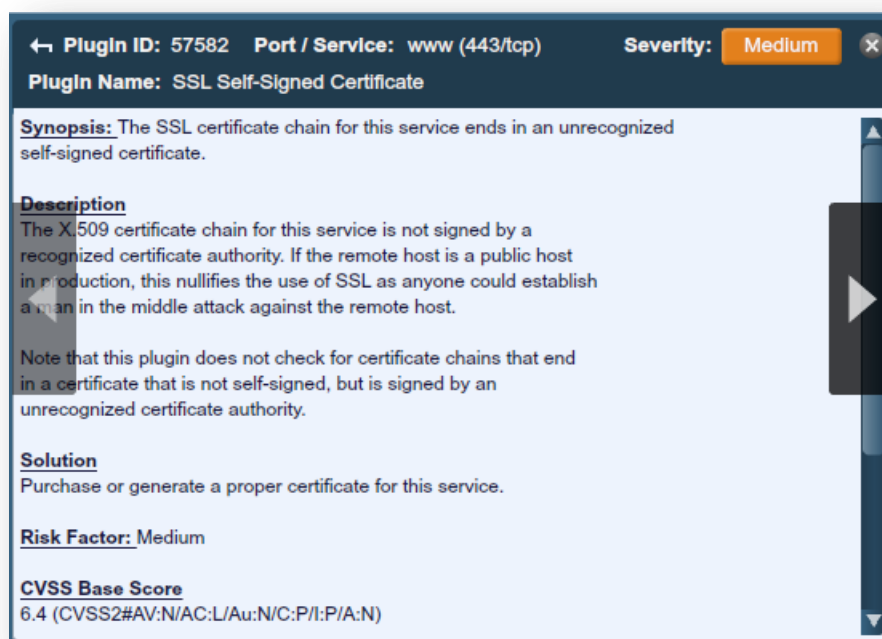
Filters | No Filters | Add Filter | Clear Filters

Host	Port	Protocol	SVC Name	Vulnerabilities
172.20.5.26	443	tcp	www	2 12 11
172.20.5.25	80	tcp	www	2 7 5
172.20.5.28	8834	tcp	www	2 9
172.20.5.60	1241	tcp	nessus	2 6
172.20.5.81	53	udp	dns	2
172.20.5.27	0	tcp	general	9
172.20.5.16	445	tcp	cifs	6
172.20.5.30	389	tcp	ldap	3
172.20.5.32	3268	tcp	ldap	3
172.20.5.31	53	tcp	dns	2
172.20.5.90	88	tcp	kerberos?	2
172.20.5.22	135	tcp	epmap	2
172.20.5.40	139	tcp	smb	2
172.20.5.63	593	tcp	http-rpc-epmap	2

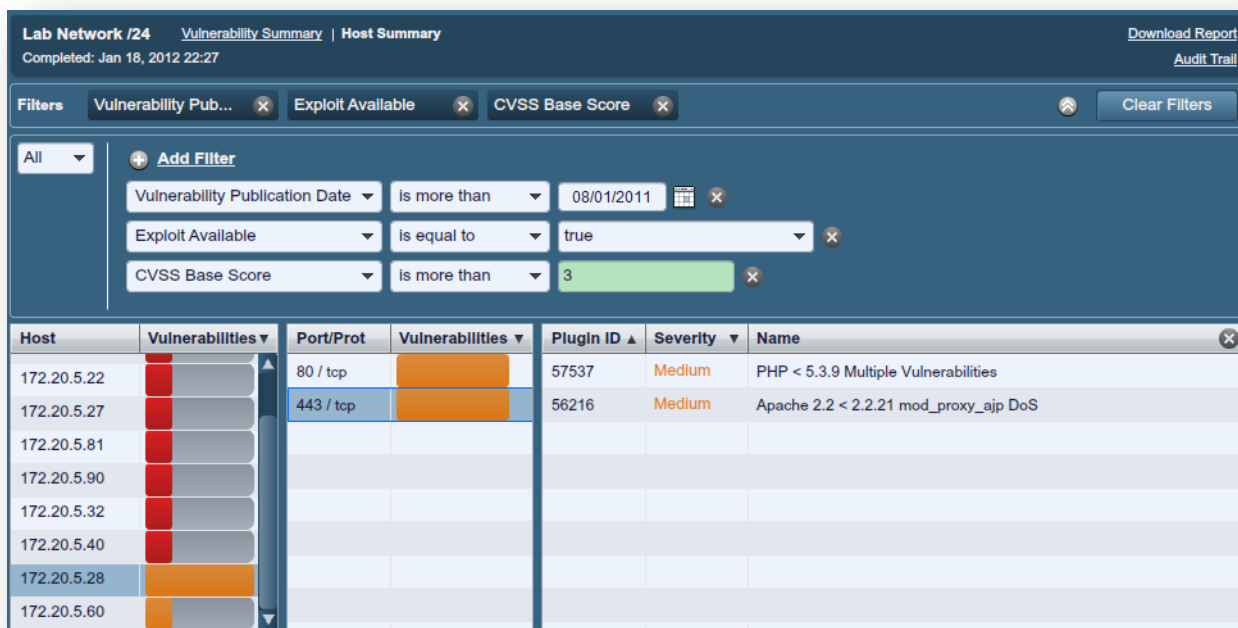
No exemplo acima, observa-se que o host 172.20.5.60 possui 30 vulnerabilidades e 82 plugins informativos associados. Para cada porta, o protocolo, nome do serviço e uma representação colorida das vulnerabilidades associadas à porta é exibida. Ao clicar uma vez em qualquer título de coluna, os resultados podem ser classificados pelo conteúdo da coluna. Um segundo clique inverte a classificação dos resultados:

Selecione uma porta na lista para exibir a lista de vulnerabilidades associadas, juntamente com a ID do plugin e a gravidade:

Clique em uma vulnerabilidade para exibir detalhes sobre ela, incluindo um resumo, descrição, solução, referências de terceiros, fator de risco, pontuação CVSS, saída de plugin (se aplicável), um conjunto de datas relacionadas ao plugin e à vulnerabilidade e se um exploit público está disponível em alguma funcionalidade (por exemplo: quadro público ou exploit):

A tela de detalhes de vulnerabilidades possui uma seta de navegação em cada lado, que permite realçar rapidamente cada vulnerabilidade:

Filtros de relatórios

A Nessus oferece um sistema de filtros flexível para auxiliar na exibição de resultados específicos do relatório. Os filtros podem ser usados para exibir os resultados de acordo com qualquer aspecto dos resultados de vulnerabilidades. Quando vários filtros forem usados, é possível criar exibições mais detalhadas e personalizadas dos relatórios.

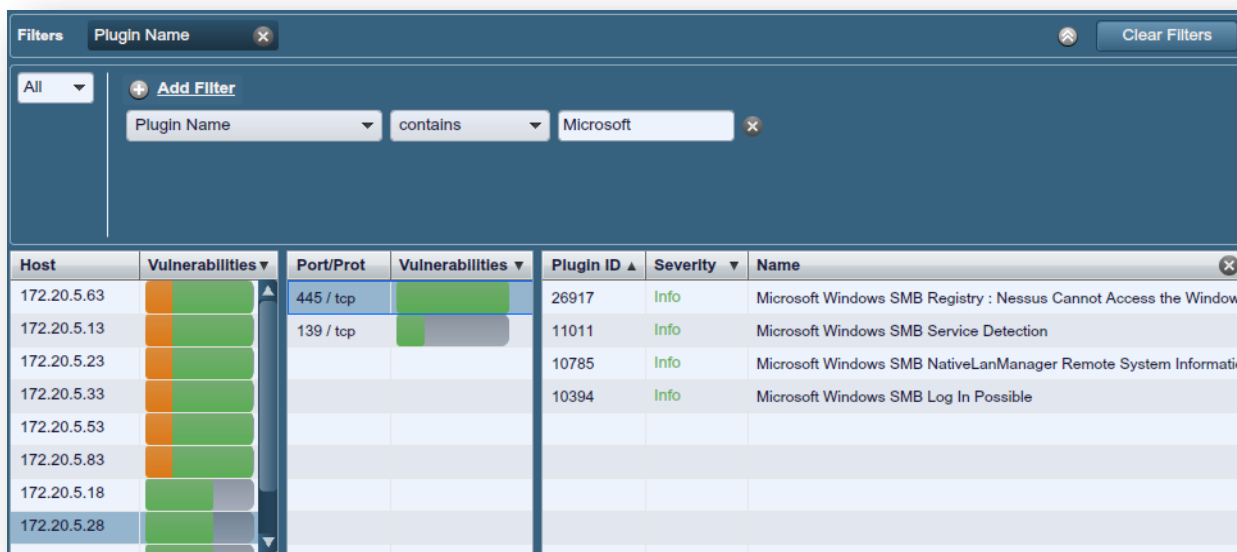
Para criar um filtro, comece clicando em "**Add Filter**" (Agregar filtro)acima dos resultados de relatórios. Os filtros podem ser criados pelas telas de resumo de relatório, host ou subdivisão em nível de porta. Vários filtros podem ser criados com lógica que permite a filtragem complexa. Um filtro é criado ao selecionar o atributo de plugin, argumento de filtro e um valor de filtragem: Ao selecionar diversos filtros, a palavra-chave "Any" ou "All" deve ser especificada corretamente. Se "All" for selecionado, todos os resultados correspondentes aos filtros **all** (todos) serão exibidos:

Depois de ter sido definido, o filtro pode ser removido individualmente ao clicar na à direita ou no botão de filtro acima. Além disso, todos os filtros podem ser removidos ao mesmo tempo ao selecionar "Clear Filters" (Despejar filtros). Os filtros de relatório aceitam uma grande variedade de critérios para controle granular dos resultados:

Opção	Descrição
Plugin ID **(ID do plugin)**	Filtra os resultados se as opções de Plugin ID forem "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: 42111).
Plugin Description **(Descrição do plugin)**	Filtra os resultados se as opções de Plugin Description forem "*contains*" (contém) ou "*does not contain*" (não contém) para uma determina string (por exemplo: "remote").
Plugin Name **(Nome do plugin)**	Filtra os resultados se as opções de Plugin Name forem "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "*windows*").
Plugin Family **(Família de plugins)**	Filtra os resultados se as opções de Plugin Name forem "is equal to" (igual a), "is not equal to" (diferente) para as famílias de plugin do Nessus designadas. As correspondências possíveis estão disponíveis no menu suspenso.
Plugin Output **(Saída de plugin)**	Filtra os resultados se as opções de Plugin Description forem "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "PHP").
Plugin Type **(Tipo de plugin)**	Filtra os resultados se as opções de Plugin Type forem "*is equal to*" (igual a), "*is not equal to*" (diferente) para um dos dois tipos de plugins: local ou remoto.
Solution **(Solução)**	Filtra os resultados se as opções de Plugin Solution forem "*contains*" (contém) ou "*does not contain*" (não contém) para uma determina string (por exemplo: "upgrade").

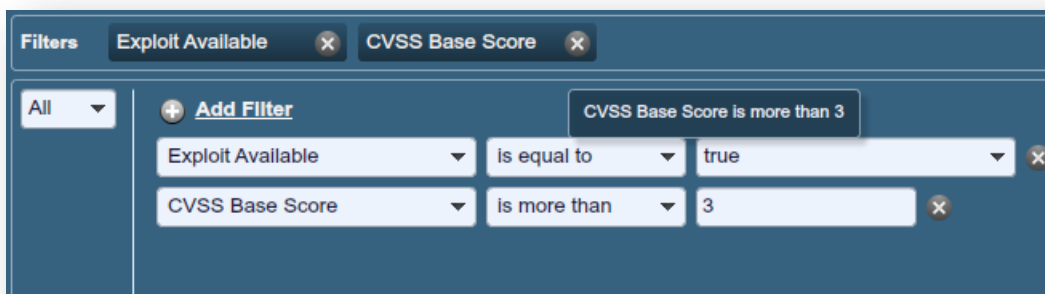
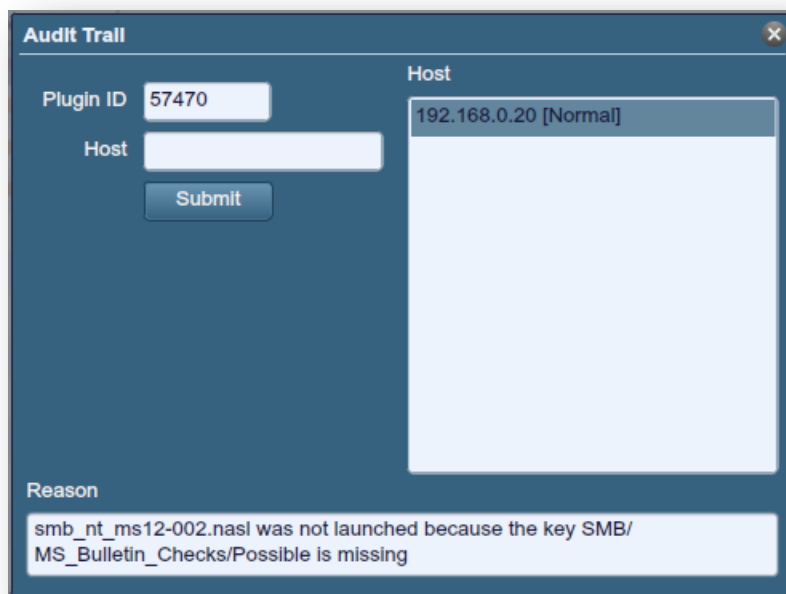
Synopsis (Sinopse)	Filtra os resultados se as opções de Solution forem "*contains*" (contém) ou "*does not contain*" (não contém) para uma determina string (por exemplo: "PHP").
Hostname (Nome do host)	Filtra os resultados se as opções de host forem "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "192.168" ou "lab").
Port (Porta)	Filtra os resultados se as opções de porta forem "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "80").
Protocol (Protocolo)	Filtra os resultados se as opções de protocolo"*is equal to*" (igual a), "*is not equal to*" (diferente) para uma determinada string (por exemplo: "http")
CPE	Filtra os resultados se as opções de Common Platform Enumeration (CPE) forem "is equal to" (igual a), "is not equal to" (diferente), "contains" (contém) ou "does not contain" (não contém) para uma determinada string (por exemplo: "solaris").
CVSS Base Score (Pontuação CVSS base)	Filtra os resultados se as opções de CVSS base score) forem "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "5"). Este filtro pode ser usado para selecionar o nível de risco. As classificações de gravidade são derivadas da respectiva pontuação CVSS, em que 0 é "Info", inferior a 4 é "Low" (baixo), inferior a 7 é "Medium" (médio), inferior a 10 é "High" (alto) e uma pontuação CVSS igual a 10 será indicada como "Critical" (grave).
CVSS Temporal Score (Pontuação CVSS temporal)	Filtra os resultados se as opções de CVSS temporal score) forem "*is less than*" (menor que), "*is more than*" (maior que), "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "3.3").
CVSS Temporal Vector (Vector CVSS temporal)	Filtra os resultados se as opções de CVSS temporal vector forem "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "E:F").
CVSS Vector (Vector CVSS)	Filtra os resultados se as opções de CVSS vector forem "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém) para uma determinada string (por exemplo: "AV:N").
Vulnerability Publication Date (Data de publicação da vulnerabilidade)	Filtra os resultados com base na data de publicação da vulnerabilidade "*earlier than*" (inferior a), "*later than*" (superior a), "*on*" (em), "*not on*" (não em), "*contains*" (contém) ou "*does not contain*" (não contém) para um string (por exemplo: "01/01/2012"). Nota: O pressionamento do botão próximo à data abrirá a interface do calendário para facilitar a escolha da data.
Patch Publication Date (Data de publicação do patch)	Filtra os resultados com base na data de publicação do plugin do Nessus com as opções "*is less than*" (menor que), "*is more than*" (maior que), "*is equal to*" (igual a), "*is not equal to*" (diferente), "*contains*" (contém) ou "*does not contain*" (não contém)

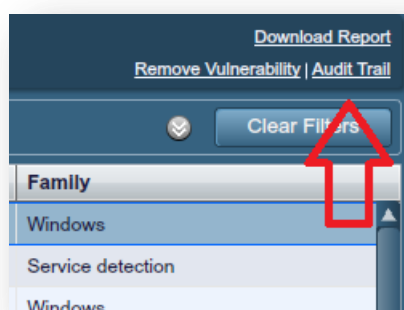
	para a string (por exemplo: “01/12/2011”).
Plugin Publication Date (Data de publicação do plugin)	Filtra os resultados com base na data de publicação do plugin do Nessus com as opções “*is less than*” (menor que), “*is more than*” (maior que), “*is equal to*” (igual a), “*is not equal to*” (diferente), “*contains*” (contém) ou “*does not contain*” (não contém) para a string (por exemplo: “03/06/2011”).
Plugin Publication Date (Data de modificação do plugin)	Filtra os resultados com base na data de modificação do plugin do Nessus com as opções “*is less than*” (menor que), “*is more than*” (maior que), “*is equal to*” (igual a), “*is not equal to*” (diferente), “*contains*” (contém) ou “*does not contain*” (não contém) para a string (por exemplo: “14/02/2010”).
CVE	Filtra os resultados se as opções de CVE reference forem “is equal to” (igual a), “is not equal to” (diferente), “contains” (contém) ou “does not contain” (não contém) para uma determinada string (por exemplo: “2011-0123”).
Bugtraq ID	Filtra os resultados se as opções de Bugtraq ID forem “is equal to” (igual a), “is not equal to” (diferente), “contains” (contém) ou “does not contain” (não contém) para uma determinada string (por exemplo: “51300”).
CERT Advisory ID (ID de aviso CERT)	Filtra os resultados se as opções de CERT Advisory ID (também chamado de Technical Cyber Security Alert) forem “is equal to” (igual a), “is not equal to” (diferente), “contains” (contém) ou “does not contain” (não contém) para uma determinada string (por exemplo: “TA12-010A”).
OSVDB ID	Filtra os resultados se a ID de Open Source Vulnerability Database (OSVDB) for “*is equal to*” (igual a), “*is not equal to*” (diferente), “*contains*” (contém) ou “*does not contain*” (não contém) para uma determinada string (por exemplo: “78300”).
Secunia ID	Filtra os resultados as opções de Secunia ID forem “*is equal to*” (igual a), “*is not equal to*” (diferente), “*contains*” (contém) ou “*does not contain*” (não contém) para uma determinada string (por exemplo: “47650”).
Exploit Database ID (ID do banco de dados de Exploit)	Filtra os resultados se a referência de Exploit Database ID (EBD-ID) for “*is equal to*” (igual a), “*is not equal to*” (diferente), “*contains*” (contém) ou “*does not contain*” (não contém) para uma determinada string (por exemplo: “18380”).
Metasploit Name (Nome do metasploit)	Filtra os resultados se as opções de Metasploit name forem “*is equal to*” (igual a), “*is not equal to*” (diferente), “*contains*” (contém) ou “*does not contain*” (não contém) para uma determinada string (por exemplo: “xslt_password_reset”).
Exploit Hub (Concentração de exploit)	Filtra os resultados se o exploit de ExploitHub for “true” (verdadeiro) ou “false” (falso).
IAVA	Filtra os resultados se a referência de IAVA for “*is equal to*” (igual a), “*is not equal to*” (diferente), “*contains*” (contém) ou “*does not contain*” (não contém) para uma determinada string (por exemplo: 2012-A-0008).
See Also (Ver também)	Filtra os resultados se a referência “*see also*” (ver também) de plugins do Nessus for “is equal to” (igual a), “*is not equal to*” (diferente), “contains” (contém) ou “*does not contain*” (não contém) para uma determinada string (por exemplo: “seclists.org”).

Exploits Available (Exploits disponíveis)	Filtra os resultados se a vulnerabilidade tiver uma exploração pública conhecida.
Exploitability Ease (Facilidade de exploração)	Filtra os resultados se as opções de facilidade exploração forem *"is equal to" (igual a), "is not equal to" (diferente) para os seguintes valores: Exploits are available" (exploits disponíveis), "No exploit is required" (não requer exploits) ou "No known exploits are available" (nenhum exploit disponível).*
Metasploit Exploit Framework (Quadro Metasploit Exploit)	Filtra os resultados com base na presença de uma vulnerabilidade no quadro Exploit Metasploit "is equal to" (igual a) verdadeiro ou falso.

Quando um filtro é usado, é possível delimitar o string ou o valor numérico por vírgulas para filtrar com base em vários strings. Por exemplo: para filtrar os resultados de maneira a exibir apenas os servidores da Web, é preciso criar um filtro "Ports", selecionar "is equal to" e inserir "80,443,8000,8080". Isto exibirá os resultados associados a essas quatro portas.

Os critérios de filtragem **não** distinguem maiúsculas e minúsculas.

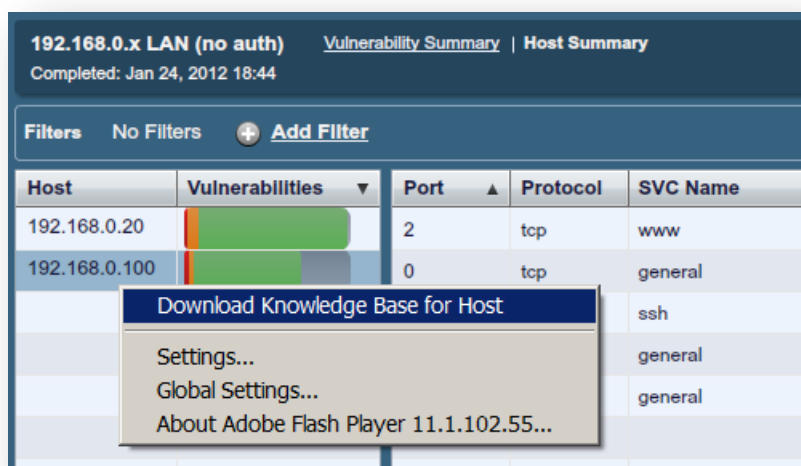
Se uma opção de filtro não estiver disponível, significa que o relatório não contém nenhuma opção que corresponde aos critérios. Por exemplo: se "Microsoft Bulletin" não estiver na listagem de filtros, nenhuma vulnerabilidades referente a um boletim da Microsoft foi encontrado.

À medida que os filtros são criados, são listados na área de entrada do filtro. Para visualizar os detalhes dos filtros ativos, passe o mouse sobre o nome de cada filtro:

Quando um filtro é criado, os resultados da varredura são atualizados para refletir os novos critérios de filtragem. No exemplo abaixo, a criação de um filtro para exibir apenas os resultados com “Microsoft” no nome do plugin excluirá a maioria dos resultados:

Depois que os resultados forem filtrados para gerar o conjunto de dados desejado, clique em “**Download Report**” (Descarregar relatório) para exportar apenas os resultados filtrados. Para receber um relatório com todos os resultados, use o botão de download na tela “**Reports**” (Relatòrios) principal.

Os resultados de varredura do Nessus fornecem uma lista concisa dos plugins detectados com problema no host. No entanto, às vezes é necessário saber porque um plugin não enviou resultados. A funcionalidade “Audit Trail” (Trilha de auditoría) fornecerá essas informações. Comece clicando em “Audit Trail” (Trilha de auditoría) no canto superior direito:

Isto abrirá a caixa de diálogo Audit Trail (Trilha de auditoría). Digite a ID do plugin do qual deseja obter mais informações. Clique no botão “Submit” (Enviar) para exibir uma série ou lista de hosts relativos à consulta. Opcionalmente, é possível fornecer um IP do host para a consulta inicial para limitar os resultados de um destino de interesse. Quando o(s) host(s) for(em) exibido(s), clique em um host para exibir informações sobre a causa da falha do plugin:

Devido aos recursos necessários para a trilha de auditoria, em alguns casos, apenas uma trilha de auditoria parcial será fornecida. A trilha de auditoria completa está disponível para um único host verificado. Se entre 2 e 512 hosts forem verificados, uma trilha de auditoria completa estará disponível somente se o servidor Nessus tiver mais de uma CPU e 2G de memória RAM. A varredura superior a 512 hosts sempre resultará em uma trilha de auditoria parcial.

Com o Nessus 5, uma Knowledge Base (KB) (Base de Conhecimento) é salva com cada varredura realizada. Este é um arquivo de texto ASCII que contém um registro de informações correspondentes para a varredura realizada e os resultados encontrados. Uma base de conhecimento é normalmente útil nos casos em que é necessário suporte da Tenable, uma vez que permite que a equipe de suporte entenda exatamente o comportamento do Nessus e as informações encontradas.

Para baixar o KB, clique com o botão direito no nome do host e selecione “Download Knowledge Base for Host” (Descarregar base de conhecimento para Host):

Compare (Comparar)

Com o Nessus, é possível comparar dois relatórios de varredura para exibir as diferenças. A capacidade de exibir as diferenças de varredura ajuda a indicar as mudanças de um determinado sistema ou rede ao longo do tempo. Isto permite analisar a conformidade ao mostrar como as vulnerabilidades são corrigidas, se os sistemas recebem correções à medida que novas vulnerabilidades são encontradas ou se duas varreduras estão direcionadas aos mesmos hosts.

Para comparar relatórios, selecione um varredura na lista “**Reports**” (Relatórios) e clique em “**Compare**” (Comparar) na barra de menus à direita. O menu de diálogo resultante exibirá uma lista suspensa de outros relatórios para comparar. Selecione um e clique em “**Submit**” (Enviar):

O Nessus irá comparar o primeiro relatório selecionado com o segundo e produzir uma lista de resultados diferentes do primeiro. O recurso de comparação mostra o que há de novo na linha de base (ou seja, o primeiro relatório selecionado), mas não produz um diferencial de dois relatórios. A comparação destaca as vulnerabilidades descobertas e corrigidas entre as duas varreduras. No exemplo acima, “LAN Scan One” é a varredura completa da sub-rede 192.168.0.0/24 e “LAN Scan Two” é a varredura nos três hosts selecionados na sub-rede 192.168.0.0/24. O recurso “Compare” exibe as diferenças ao realçar os hosts verificados em “LAN Scan Two”:

A função "Compare" (Comparar) está disponível apenas para os usuários do ProfessionalFeed.

Upload e download (Carregar e descarregar)

Os resultados das varreduras podem ser exportados de um scanner Nessus e importados para outro scanner Nessus. Os recursos "**Upload**" (Carregar) e "**Download**" (Descarregar) facilitam o gerenciamento das varreduras, comparação de relatórios, backup de relatórios e a comunicação entre grupos ou organizações em uma empresa.

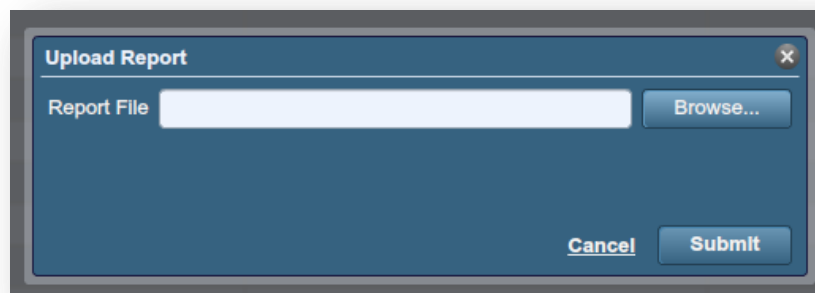
Para exportar uma varredura, selecione-a na tela "**Reports**" (Relatórios) e clique em "**Download**" (Descarregar). Isto exibirá a caixa de diálogo de download do relatório que o formato desejado, bem como informações específicas (divididas em "capítulos") que devem ser incluídos. Clique no capítulo desejado para exibir uma marca de verificação para indicar que será incluído no relatório:

As varreduras de conformidade realizadas com o Nessus 5 podem ser exportadas para os formatos PDF ou HTML com os capítulos de conformidade. As varreduras importadas de versões anteriores do Nessus não serão exportadas desta maneira.

Os relatórios podem ser baixados em vários formatos. Observe que alguns formatos não permitirão a seleção de capítulos ou incluirão todas as informações.

Opção	Descrição
`.nessus`	Um formato do tipo XML, padrão do Nessus 4.2 e versões posteriores. Este formato usa um conjunto extenso de tags XML, que tornam a extração e a análise de informações mais granular. Este relatório não permite selecionar o capítulo.
`.nessus` **(v1)**	Um formato do tipo XML usado do Nessus 3.2 ao 4.0.2, compatível com o Nessus 4.x e Security Center 3. Este relatório não permite selecionar o capítulo.
HTML	Relatório com gerado em HTML padrão que permite selecionar o capítulo. Este relatório será aberto em uma nova guia do navegador.
PDF	Relatório com gerado formato PDF que permite selecionar o capítulo. Dependendo do tamanho do relatório, a geração de PDF pode levar vários minutos. O Oracle Java (conhecido como Java da Microsystems) é necessário para a funcionários de relatórios no formato PDF.
CSV	Exportação em valores separados por vírgulas, que pode ser usada para importação em muitos programas externos, como bancos de dados, planilhas e outros. Este relatório não permite selecionar o capítulo.
NBE export	Exportação delimitada por barras verticais, que pode ser usada para importação em muitos programas externos. Este relatório não permite selecionar o capítulo.

Depois de selecionar o formato `.nessus`, NBE ou PDF, a caixa de diálogo "Save File" (Salvar Arquivo) do navegador será exibida, permitindo que o usuário salve os resultados da varredura no local de sua escolha. Os relatórios em HTML são exibidos no navegador e podem ser salvos com a função "File -> Save" ("Arquivo > Salvar").

Para importar um relatório, clique no botão "**Upload Report**" (Carregar relatório) no lado superior esquerdo da tela "**Reports**" (Relatórios):

Com o botão "**Browse...**" (Procurar), selecione o arquivo de varredura .nessus que deseja importar e clique em "**Submit**" (Enviar). O Nessus analisará as informações e as disponibilizará na interface "**Reports**" (Relatórios).

Formato de arquivo .nessus

O Nessus usa um formato de arquivo específico (.nessus) para importar e exportar varreduras. Este formato tem as seguintes vantagens:

- É um arquivo do tipo XML compatível com versões anteriores e futuras e facilita a implementação.
- Autossuficiente: um único arquivo .nessus contém a lista de alvos e as políticas definidas pelo usuário, além dos próprios resultados da varredura.
- Seguro: as senhas não são salvas no arquivo. Em vez disso, usa-se uma referência a uma senha armazenada em um local seguro no host local.

O processo de criação de um arquivo **`.nessus`** que contém os alvos, as políticas e os resultados das varreduras é, primeiramente, gerar a política e salvá-la. Em seguida, gerar a lista de endereços de destino e, por último, executar uma varredura. Quando a varredura for concluída, todas as informações podem ser salvas em um arquivo **`.nessus`** com a opção "**Download**" (Descarregar) da guia "**Reports**" (Relatórios). Consulte o documento "Formato de Arquivo Nessus" para obter mais detalhes sobre os arquivos **`.nessus`**.

Delete (Excluir)

Quando os resultados da varredura forem concluídos, selecione um varredura na lista "Reports" e clique no botão "**Delete**" (Excluir). Isto excluirá a varredura da interface do usuário. **Essa ação não pode ser desfeita.** Use o recurso "**Download**" (Descarregar) para exportar os resultados de varredura antes da exclusão.

Mobile (Móvel)

O Nessus 5 tem capacidade para examinar Active Directory Service Interfaces e Apple Profile Manager, permitindo o exame de inventário e vulnerabilidades de dispositivos baseados em Apple iOS e Android. O Nessus pode ser configurado para autenticar nesses servidores, consultar informações de dispositivos móveis e reportar questões. Isso pode ser feito com uma política de varreduras tradicional ou com a guia "**Mobile**" (Móvel).

Para procurar dispositivos móveis, o Nessus deve ser configurado com informações de autenticação para o servidor de gerenciamento e/ou os plugins móveis de interesse.

Como o Nessus autentica diretamente nos servidores de gerenciamento, uma política de varreduras não precisa ser configurada para examinar hosts específicos.

A guia "Mobile" (Móvel) oferece um lugar único para configurar as informações de Apple Profile Manager e ADSI. Depois que os detalhes forem adicionados e enviados, o Nessus examinará esses servidores imediatamente para recuperar informações de dispositivos móveis. Clicar nesta guia novamente reiniciará uma varredura para obter informações atualizadas.

As únicas informações necessárias para iniciar um exame de dispositivo móvel básico são as informações do servidor Active Directory (Diretório ativo) ou MDM. Quando essas informações estiverem completas, um exame começará e os resultados poderão ser visualizados na guia “**Reports**” (Relatórios).

SecurityCenter

Configuração do SecurityCenter 4.0-4.2 para funcionar com o Nessus

O “Nessus Server” pode ser adicionado por meio da interface de administração do SecurityCenter. Usando essa interface, o SecurityCenter pode ser configurado para acessar e controlar praticamente qualquer scanner Nessus. Clique na guia “Resources” (Recursos) e, em seguida, clique em “**Nessus Scanners**”. Clique em “**Add**” (Adicionar) para abrir a caixa de diálogo “Add Scanner” (Adicionar Scanner). O endereço IP do scanner Nessus, a porta do Nessus (padrão: 1241), o ID de login administrativo, o tipo de autenticação e a senha (criada durante a configuração do Nessus) são obrigatórios. Os campos de senha não estarão disponíveis se a autenticação “SSL Certificate” (Certificado SSL) for selecionada. Além disso, as zonas às quais o scanner Nessus será atribuído podem ser selecionadas.

Um exemplo de imagem da página “Add Scanner” (Adicionar Scanner) do SecurityCenter é mostrado abaixo:

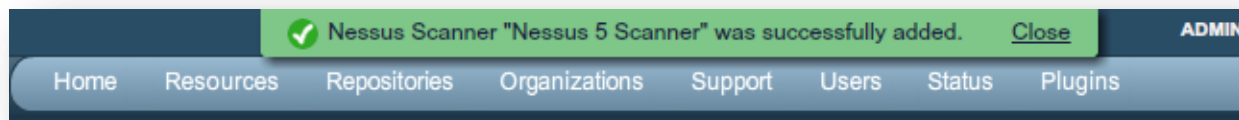
Depois de adicionar com êxito o scanner, a seguinte página é exibida após a seleção do scanner:

Consulte mais informações no “Guia de Administração do SecurityCenter”.

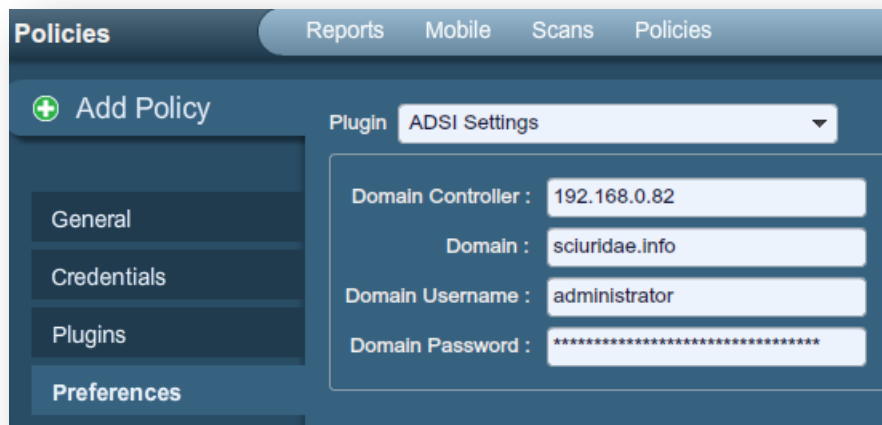
Configuração do SecurityCenter 4.4 para funcionar com o Nessus

A interface de administração do SecurityCenter é usada para configurar o acesso e controlar qualquer scanner Nessus, ou seja, versão 4.2.x ou superior. Clique na guia “**Resources**” (Recursos) e, em seguida, clique em “**Nessus Scanners**”. Clique em “**Add**” (Adicionar) para abrir a caixa de diálogo “**Add Scanner**” (Adicionar Scanner). O endereço IP ou nome do host do scanner Nessus, a porta do Nessus (padrão: 8834), as informações sobre o tipo de autenticação (criado durante a configuração do Nessus), a ID de login administrativo e a senha são obrigatórios. Os campos de senha não estarão disponíveis se a autenticação “SSL Certificate” (Certificado SSL) for selecionada. A capacidade de verificar o nome do host é fornecida para verificação do CommonName (CN) do certificado SSL apresentado pelo servidor Nessus. O estado do scanner Nessus pode ser definido como ativado ou desativado, conforme o necessário (ativado é o padrão). As áreas do scanner Nessus podem ser atribuídas para seleção.

Um exemplo de imagem da página **“Add Scanner”** (Adicionar Scanner) do SecurityCenter 4.4 é mostrado abaixo:

Depois de adicionar o scanner com êxito, o banner a seguir é exibido:

Para obter mais informações sobre como integrar o Nessus ao SecurityCenter, consulte “Guia de Administração do SecurityCenter”.

Firewalls instalados no host

Se o servidor Nessus estiver configurado com um firewall local como ZoneAlarm, Sygate, BlackICE, firewall do Windows XP ou qualquer outro software de firewall, será necessário que as conexões sejam permitidas a partir do endereço IP do SecurityCenter.

Normalmente, a porta 8834 é usada. Nos sistemas Microsoft XP Service Pack 2 (SP2) e posteriores, clique em **“Security Center”** (Central de Segurança) no “**Control Panel**” (Painel de Controle) para gerenciar as configurações da opção “Firewall do Windows”. Para abrir a porta 8834, selecione a guia **“Exceptions”** (Exceções) e adicione a porta “8834” à lista.

Se o SecurityCenter usar o protocolo NTP obsoleto por meio da porta 1241, os comandos acima usariam 1241 em vez de 8834.

Verificação de preferências detalhadas

A guia “**Preferences**” (Preferências) contém 40 menus de controle individualizados para configuração de varreduras. Recomenda-se reservar algum tempo para explorar e configurar cada menu para obter mais flexibilidade e resultados de verificação mais precisos com relação à política padrão. A seção a seguir oferece mais detalhes sobre cada opção “**Preferences**” (Preferências). Observe que esta é uma lista dinâmica de opções de configuração e depende do feed de plugins, das políticas de auditoria e de outras funções às quais o scanner Nessus conectado tem acesso. Um scanner com ProfessionalFeed pode ter opções de configuração mais avançadas do que um scanner configurado com o HomeFeed. Esta lista também pode mudar à medida que os plugins são adicionados ou modificados.

“**ADSI Settings**” (Configurações ADSI) permite que o Nessus consulte um servidor ActiveSync para determinar se algum dispositivo Android ou iOS está conectado. Usando as credenciais e as informações de servidor, o Nessus autentica no controlador de domínio (não no servidor Exchange) para consultá-lo diretamente sobre informações de dispositivos. Esse recurso não exige que quaisquer portas sejam especificadas na política de varredura. Essas configurações são obrigatórias para varreduras de dispositivos móveis.

Nota: Para “ADSI Settings” (Configurações ADSI) e “Apple Profile Manager API Settings” (Configurações da API do Apple Profile Manager), os dispositivos host não precisam ser examinados diretamente para obtenção de informações. O scanner Nessus deve ser capaz de alcançar o servidor MDM para consultá-lo quanto a informações. Quando uma dessas opções está configurada, a política para varreduras não exige um host de destino; você pode apontar para “localhost” e a política ainda conectará com o servidor MDM para obter informações.

"**Apple Profile Manager API Settings**" (Configurações da API do Apple Profile Manager) permite que o Nessus consulte um servidor Apple Profile Manager para enumerar dispositivos baseados em Apple iOS (por exemplo, iPhone, iPad) na rede. Usando as credenciais e as informações de servidor, o Nessus autentica no Profile Manager para consultá-lo diretamente sobre informações de dispositivos. Ou então, é possível especificar comunicações por SSL, assim como direcionar o servidor para forçar uma atualização de informações de dispositivos (ou seja, cada dispositivo atualizará suas informações no servidor do Profile Manager).

Esse recurso não exige que quaisquer portas sejam especificadas na política de varredura. Essas configurações são obrigatórias para varreduras de dispositivos móveis.

"**Cisco IOS Compliance Checks**" (Verificações de conformidade de Cisco IOS) permite que os clientes do ProfessionalFeed enviem arquivos de políticas que serão usados para determinar se um dispositivo Cisco IOS verificado cumpre as normas de conformidade especificadas. Até cinco políticas podem ser selecionadas ao mesmo tempo. As políticas podem aplicadas com base nas configurações Saved (Salvo) (`show config`), Running (Em Execução) (`show running`) ou Startup (Inicialização) (`show startup`).

“**Database Compliance Checks**” (Verificações de conformidade de banco de dados) permite que os clientes do ProfessionalFeed enviem arquivos de políticas que serão usados para determinar se um banco de dados testado cumpre as normas de conformidade especificadas. Até cinco políticas podem ser selecionadas ao mesmo tempo.

As opções “**Database settings**” (Configurações de banco de dados) são usadas para especificar o tipo de banco de dados a ser verificado e as configurações e credenciais correspondentes:

Opção	Descrição
Login	Nome de usuário do banco de dados.
Password (Senha)	A senha para o nome de usuário fornecido.
DB Type (Tipo de DB)	Oracle, SQL Server, MySQL, DB2, Informix/DRDA e PostgreSQL são permitidos.
Database SID (SID de banco de dados)	ID do banco de dados para auditoria.

Database port to use (Porta do banco de dados para usar)	Porta de escuta do banco de dados.
Oracle auth type (Tipo de aut. Oracle)	NORMAL, SYSOPER e SYSDBA são permitidos.
SQL Server auth type (Tipo de aut. SQL Server)	Windows ou SQL são permitidos.

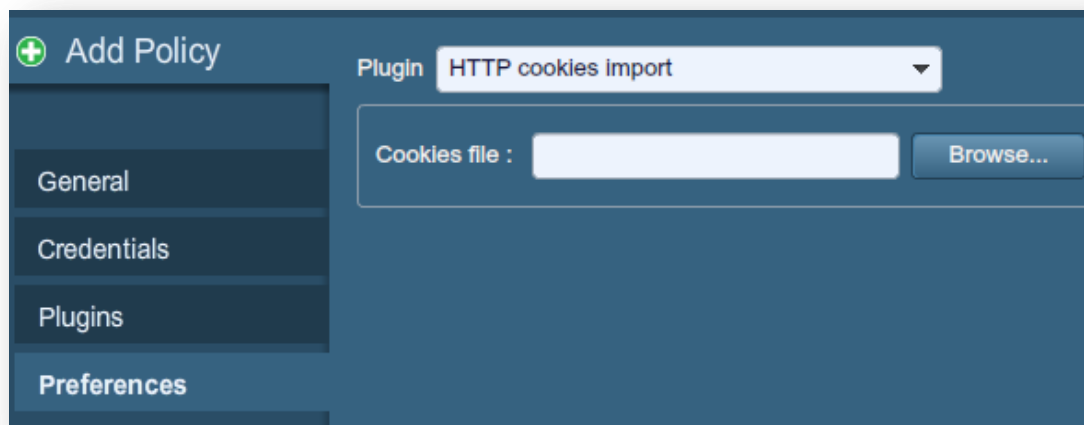
Do not scan fragile devices” (Não verificar dispositivos frágeis) oferece duas opções que instruem o scanner Nessus a não verificar um histórico de “fragilidade” ou propensão a falhas ao receber uma entrada inesperada. Os usuários podem selecionar “Scan Network Printers” (Verificar impressoras em rede) ou “Scan Novell Netware hosts” (Verificar hosts Novell Netware) para instruir o Nessus a verificar esses dispositivos específicos. O Nessus só irá verificar as opções se estiverem marcadas. Recomenda-se que a verificação desses dispositivos seja realizada de maneira que permita às equipes de TI monitorar problemas nos sistemas.

“**Global variable settings**” (Configurações de variáveis globais) contém uma grande variedade de opções de configuração para o servidor Nessus.

A tabela a seguir fornece informações detalhadas sobre cada opção disponível:

Opção	Descrição
Probe services on every port	Relaciona cada porta aberta ao serviço que está sendo executado na porta. Observe que, em alguns casos raros, isto pode prejudicar alguns serviços e causar efeitos colaterais inesperados.
Do not log in with user accounts not specified in the policy	Usado para evitar o bloqueio de contas se a política de senhas estiver definida para bloquear as contas depois de algumas tentativas inválidas.
Enable CGI scanning	Ativa a varredura de CGI. Desative esta opção para acelerar a auditoria de uma rede local.
Network type	Permite especificar se os IPs públicos roteáveis, IPs roteáveis privados não pertencentes à Internet ou uma combinação de ambos estão em uso. Selecione “Mixed” (Combinado) se os endereços RFC 1918 forem usados com diversos roteadores de rede.
Enable experimental scripts	Faz com que os plugins "em teste" sejam usados na varredura. Não ative esta opção durante a varredura de uma rede de produção.
Thorough tests (slow)	Permite que os plugins realizem testes "completos". Por exemplo: ao examinar compartilhamentos de arquivos SMB, um plugin pode analisar com três níveis de profundidade em vez de 1. Isto pode aumentar o tráfego da rede e as análises, em

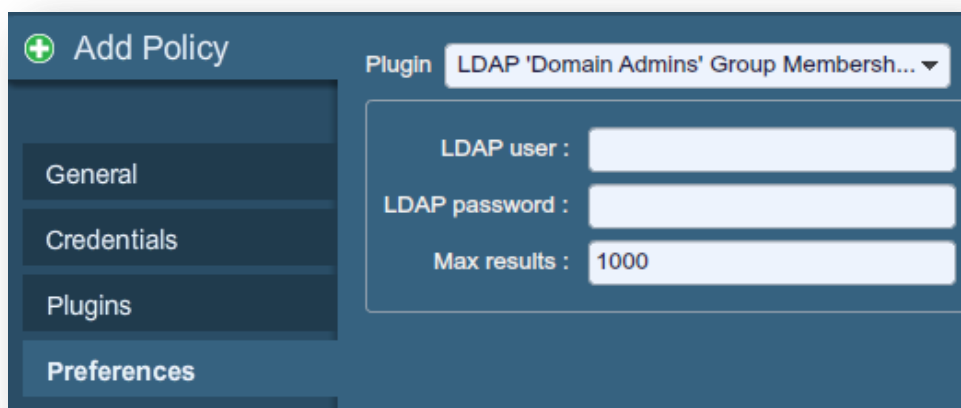
	alguns casos. Observe que, por ser mais completa, a varredura deve ser mais invasiva e é mais provável que afete a rede, mas os resultados de auditoria podem ser melhores.
Report verbosity	Um valor mais alto irá gerar mais ou menos informações sobre a atividade do plugin no relatório.
Report paranoia	Em alguns casos, o Nessus não pode determinar remotamente se uma falha está presente ou não. Se Report paranoia (Sensibilidade do relatório) for definido como "**Paranoid**" (Sensível), uma falha sempre será relatada, mesmo se houver dúvidas sobre o host remoto afetado. Por outro lado, a configuração de sensibilidade "**Avoid false alarm**" (Evitar alarmes falsos) fará com que o Nessus não comunique nenhuma falha sempre que houver uma sombra de incerteza sobre o host remoto. A opção ("**Normal**") é a configuração padrão entre as configurações acima.
HTTP User-Agent	Especifica o tipo de navegador que o Nessus representará durante a varredura.
SSL certificate to use	Permite que o Nessus use certificado SSL no lado cliente para se comunicar com um host remoto.
SSL CA to trust	Especifica a Autoridade Certificadora (CA) para confiabilidade do Nessus.
SSL key to use	Especifica uma chave SSL local que será usada para se comunicar com o host remoto.
SSL password for SSL key	A senha usada para gerenciar a chave SSL especificada.

Para facilitar os testes de aplicativos da Web, o Nessus pode importar cookies HTTP de um outro software (por exemplo: navegador, proxy de Web etc.) com as configurações "**HTTP cookies import**" (Importação de cookies HTTP). Um arquivo de cookie pode ser enviado para que o Nessus utilize cookies para acessar um aplicativo da Web. O arquivo do cookie deve estar no formato Netscape.

As configurações "**HTTP login page**" (Página de login de HTTP) permitem controlar o local em que os testes autenticados de um aplicativo de Web personalizado têm início.

Opção	Descrição
Login page	O URL básico para a página de login do aplicativo.
Login form	O parâmetro "action" do método do formulário. Por exemplo: o formulário de login de `<form method="POST" name="auth_form" action="/login.php"> deve ser "/login.php".`
Login form fields	Especifica os parâmetros de autenticação (por exemplo: Se as palavras-chaves %USER% e %PASS% forem usadas, serão substituídas por valores fornecidos no menu suspenso "Login configurations" (Configurações de login). Este campo pode ser usado para fornecer mais de dois parâmetros, se necessário (por exemplo: um nome de "grupo" ou alguma outra informação é necessária para o processo de autenticação).
Login form method	Especifica se a ação de login é realizada por meio de uma solicitação GET ou POST.
Automated login page search	Instrui o Nessus a pesquisar uma página de login.
Re-authenticate delay (seconds)	O intervalo entre as tentativas de autenticação. Previne o acionamento de mecanismos de bloqueio por força bruta.
Check authentication on page	O URL de uma página da Web protegida que requer autenticação para ajudar o Nessus a definir o status de autenticação.
Follow 30x redirections (# of levels)	Se um código de redirecionamento 30x for recebido de um servidor da Web, isso instruirá o Nessus a seguir o link fornecido ou não.
Authenticated regex	Um padrão regex para pesquisa na página de login. O recebimento de um código de resposta 200 nem sempre é suficiente para determinar o estado da sessão. O Nessus pode tentar localizar um determinado string, como "Authentication successful!" (Autenticação concluída).
Invert test (disconnected if regex matches)	Um padrão regex para pesquisa na página de login. Se for encontrado, indica ao Nessus que a autenticação não foi concluída (por exemplo: "Authentication failed!").
Match regex on HTTP headers	O Nessus pode pesquisar um determinado padrão regex nos cabeçalhos de resposta HTTP para definir melhor o estado de autenticação, ao invés de pesquisar no corpo de uma resposta.
Case insensitive regex	Normalmente, as pesquisas por regex diferenciam maiúsculas de minúsculas. O comando instrui o Nessus a ignorar a caixa.
Abort web application tests if login fails	Se as credenciais fornecidas não funcionarem, o Nessus interromperá os testes personalizados de aplicativos da Web, mas não as famílias de plugins de CGI.

“**IBM iSeries Compliance Checks**” (Verificações de conformidade IBM iSeries) permite que os clientes do ProfessionalFeed enviem arquivos de políticas que serão usados para determinar se um banco de dados testado cumpre as normas de conformidade especificadas. Até cinco políticas podem ser selecionadas ao mesmo tempo.

As preferências de “**IBM iSeries Credentials**” (Credenciais para IBM iSeries) proporciona um local para que o Nessus forneça credenciais para autenticação do sistema IBM iSeries. Isto é necessário para auditorias de conformidade, por exemplo.

O menu “**ICCP/COTP TSAP Addressing**” (Endereçamento ICCP/COTP TSAP) está relacionado especificamente às verificações Scada. O menu determina um valor de Pontos de Acesso de Serviço de Transporte (TSAP) do protocolo de Transporte Orientado a Conexões (COTP) em um servidor ICCP. Os valores de início e parada são definidos inicialmente como “8”.

O menu “LDAP ‘Domain Admins’ Group Membership Enumeration” (Enumeraçao da membresía no grupo ‘Domain Admin’ LDAP) permite inserir um conjunto de credenciais LDAP que podem ser usados para enumerar uma lista de membros do grupo “Domain Admins” no diretório LDAP remoto.

"**Login configurations**" (Configurações de Login) permite que o scanner Nessus use credenciais ao verificar HTTP, NNTP, FTP, POP2, POP3 ou IMAP. Ao fornecer credenciais, o Nessus pode realizar verificações mais abrangentes para determinar as vulnerabilidades. As credenciais de HTTP fornecidas aqui serão usadas apenas para autenticação básica e resumida. Para configurar as credenciais de um aplicativo da Web personalizado, use o menu suspenso "HTTP login page" (Página de login HTTP).

Plugin: Login configurations

HTTP account :
HTTP password (sent in clear) :
NNTP account :
NNTP password (sent in clear) :
FTP account : anonymous
FTP password (sent in clear) : *********
FTP writeable directory : /incoming
POP2 account :
POP2 password (sent in clear) :
POP3 account :
POP3 password (sent in clear) :
IMAP account :
IMAP password (sent in clear) :

As opções "**Modbus/TCP Coil Access**" (Acesso Modbus/TCP Coil) estão disponíveis para os usuários do ProfessionalFeed. Este item de menu é gerado dinamicamente pelos plugins SCADA disponíveis com o

ProfessionalFeed. O Modbus usa o código de função 1 para ler “bobinas” em um escravo Modbus. As bobinas representam configurações de saída binárias e normalmente são correlacionadas com atuadores. A capacidade de ler bobinas pode permite a um atacante criar um perfil do sistema, identificar intervalos de registros e alterá-los por meio de uma mensagem “write coil” (gravar bobina). Os valores padrão são “0” para o reg Start e “16” para o reg End.

“As opções “**Nessus SYN scanner**” e “**Nessus TCP scanner**” permitem configurar os scanners SYN e TCP originais para detectar a presença de um firewall.

Valor	Descrição
Automatic (normal)	Esta opção pode ajudar a identificar se um firewall está localizado entre o scanner e o destino (**padrão**).
Disabled (softer)	Desativa o recurso **Firewall detection** (Detecção de firewall).
Do not detect RST rate limitation (soft)	Desativa a funcionalidade de monitoramento do número de reinícios definidos e determina se há uma limitação configurada por um dispositivo de rede local.
Ignore closed ports (aggressive)	Tenta executar os plugins mesmo que a porta estiver fechada. Recomenda-se que esta opção não seja usada em uma rede de produção.

“**A opção “News Server (NNTP) Information Disclosure**” (Divulgação de Informações do Servidor de Notícias (NNTP)) pode ser usada para determinar a existência de servidores de notícias capazes de distribuir spam. O Nessus tentará

publicar uma mensagem ao(s) servidor(es) de notícias NNTP (Protocolo de Transporte de Notícias em Rede) para verificar se é possível enviar uma mensagem a servidores de notícias em um ponto da rede remota.

Opção	Descrição
From address	O endereço que o Nessus usará ao tentar enviar uma mensagem ao(s) servidor(es) de notícias. Essa mensagem será excluída automaticamente após um breve intervalo de tempo.
Test group name regex	Nome do grupo de notícias que receberá uma mensagem de teste do endereço especificado. O nome pode ser especificado como uma expressão regular (regex) para que a mensagem possa ser enviada simultaneamente a vários grupos de notícias. Por exemplo: o valor padrão "**f[a-z]\.tests?**" transmitirá uma mensagem de e-mail a todos os grupos de notícias com nomes que começam com qualquer letra (de "a" a "z") e terminam com ".tests" (ou alguma variação que corresponda ao string). O ponto de interrogação age como um caractere curinga opcional.
Max crosspost	O número máximo de servidores de notícias que receberão a publicação de teste, independentemente do número de correspondências de nomes. Por exemplo: se o crosspost Max for "**7**", a mensagem de teste será enviada apenas a sete servidores de notícias, mesmo que haja 2.000 servidores de notícias correspondentes ao regex neste campo.
Local distribution	Se esta opção for selecionada, o Nessus tentará enviar apenas uma mensagem ao(s) servidor(es) de notícias local(is). Caso contrário, tentará encaminhar a mensagem a um ponto remoto.
No archive	Se esta opção for selecionada, o Nessus solicitará para não arquivar a mensagem de teste enviada ao(s) servidor(es) de notícias. Caso contrário, a mensagem será arquivada como qualquer outra publicação.

"**Oracle Settings**" (Configurações do Oracle) configura o Nessus com o Oracle Database SID e inclui uma opção para testar contas padrão conhecidas no software da Oracle.

"**PCI DSS Compliance**" (Conformidade PCI DSS) fará com que o Nessus compare os resultados das varreduras com as normas de conformidade PCI DSS vigentes. Este recurso está disponível apenas para os clientes do ProfessionalFeed.

O Nessus pode explorar credenciais para o servidor Red Hat Satellite, WSUS, SCCM e sistemas de gerenciamento de patches VMware Go (anteriormente Shavlik) para realizar a auditoria de patches nos sistemas nos quais as credenciais não estão disponíveis para o scanner Nessus As opções dos sistemas de gerenciamento de patches "Preferences" podem ser encontrados em seus respectivos menus suspensos: **Patch Management: Red Hat Satellite Server Settings"**(Gerenciamento de patches: Configurações do servidor Red Hat Satellite)**, "Patch Management: SCCM Server Settings"**(Gerenciamento de patches: Configurações do servidor SCCM)**, "Patch Management: VMware Go Server Settings"**(Gerenciamento de patches: Configurações do servidor VMware Go) **e "Patch Management: WSUS Server Settings"**(Gerenciamento de patches: Configurações do servidor WSUS)**.** Para obter mais informações sobre como utilizar o Nessus para verificar os hosts por meio desses sistemas de gerenciamento de patch, consulte o documento "Patch Management Integration".

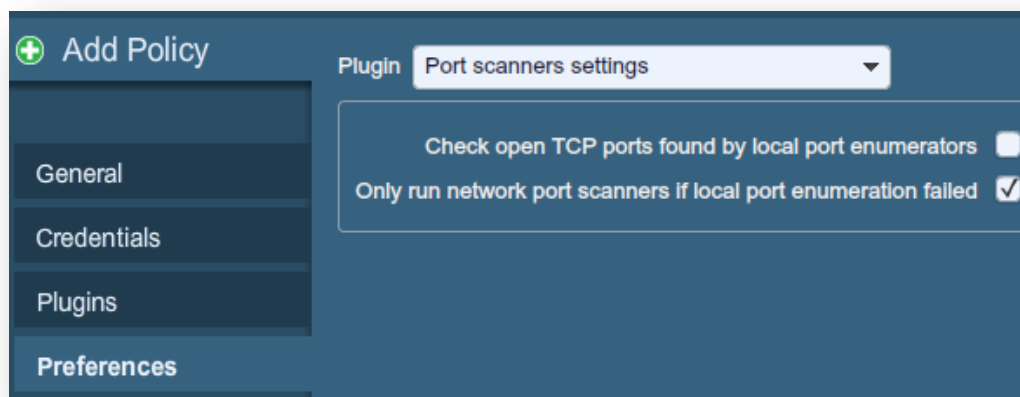
"As opções "**Ping the remote host**" (Teste de ping para o host remoto) permitem um controle individualizado sobre a capacidade do Nessus de enviar testes de conexão a hosts durante a varredura de descoberta. Isto pode ser feito com ping ARP, ping TCP, ping ICMP ou ping UDP de aplicativo.

Opção	Descrição
TCP ping destination port(s)	Especifica a lista de portas a serem verificadas por meio do teste de ping TCP. Se tiver dúvidas com relação às portas, deixe esta configuração com o valor padrão "interno".

Number of Retries (ICMP)	Permite especificar o número de tentativas de ping ao host remoto. O valor padrão é 6.
Do an applicative UDP ping (DNS, RPC…)	Executa um teste de ping UDP em aplicativos específicos que usam UDP, incluindo DNS (porta 53), RPC (porta 111), NTP (porta 123) e RIP (porta 520).
Make the dead hosts appear in the report	Se esta opção for selecionada, os hosts que não responderam à solicitação de ping serão incluídos no relatório de segurança como hosts inativos.
Log live hosts in the report	Selecione esta opção para comunicar especificamente a capacidade de enviar um ping a um host remoto.
Test the local Nessus host	Esta opção permite que o usuário inclua ou exclua o host do Nessus local da varredura. Esta opção é usada quando o host Nessus estiver dentro do intervalo de rede de destino da varredura.
Fast network discovery	Normalmente, ao enviar um "ping" a um IP remoto com uma resposta, o Nessus realiza varreduras adicionais para verificar se não se trata de um proxy transparente ou um balanceador de carga gerando ruído, mas sem resultado (alguns dispositivos respondem a todas as portas de 1 a 65.535, mas não há nenhum serviço em segundo plano). As verificações podem demorar um pouco, especialmente se o host remoto estiver protegido por um firewall. Se a "descoberta rápida de rede" estiver ativada, o Nessus não realizará as varreduras.

Para examinar os sistemas VMware convidados, o "ping" deve ser desativado. Na política de varredura em "Advanced" (Avançado) -> "Ping the remote host" (Ping para o host remoto), desmarque o ping de TCP, ICMP e ARP.

"**Port scanner settings**" (Configurações do scanner de portas) oferece duas opções adicionais para controlar a atividade de varredura de portas:

Opção	Descrição
Check open TCP ports found by local port enumerators	Se um enumerador de portas locais (por exemplo: WMI ou netstat) encontrar uma porta, o Nessus também verificará se está aberta remotamente. Isto ajuda a determinar se alguma forma de controle de acesso está em uso (por exemplo: TCP wrappers, firewall).
Only run network port scanners if local port enumeration failed	Nesse caso, use primeiro a enumeração de portas locais.

"**SMB Registry: Start the Registry Service during the scan**" (Registro de SMB: Iniciar o Serviço de Registro durante a varredura) permite que o serviço intermedeie algumas das exigências de varredura para computadores em que o registro SMB não funcione todo o tempo.

No menu "**SMB Scope**" (Escopo de SMB), se a opção "**Request information about the domain**" (Solicitar informações sobre o domínio) estiver selecionada, os usuários do domínio, e não os usuários locais, serão consultados.

“**SMB Use Domain SID to Enumerate Users**” (SMB usa o SID de Domínio para Enumerar Usuários) especifica o intervalo de SID a ser usado para realizar uma consulta inversa de nomes de usuários no domínio. A configuração padrão é recomendada para a maioria das varreduras.

“**SMB Use Host SID to Enumerate Local Users**” (SMB usa o SID de Host para Enumerar Usuários) especifica o intervalo de SID a ser usado para executar uma consulta inversa de nomes de usuários locais. A configuração padrão é recomendada.

"**SMTP settings**" (Configurações de SMTP) especifica as opções para os testes de SMTP (Protocolo Simples de Transporte de Correio) executados em todos os dispositivos dentro do domínio verificado que estão executando serviços SMTP. O Nessus tentará retransmitir mensagens por meio do dispositivo ao domínio de terceiros especificado ("**Third party domain**"). Se a mensagem enviada ao domínio de terceiros especificado for recusada pelo endereço especificado no campo "**To address**" (Endereço de destino), ocorrerá falha na tentativa de spam. Se a mensagem for aceita, o servidor de SMTP foi usado com sucesso para retransmitir o spam.

Opção	Descrição
Third party domain	O Nessus tentará enviar spam por meio de cada dispositivo de SMTP para o endereço listado neste campo. O endereço de domínio de terceiros deve estar fora do intervalo do site que está sendo examinado ou do site que está realizando a varredura. Caso contrário, o teste pode ser interrompido pelo servidor SMTP.
From address	As mensagens de teste enviadas ao(s) servidor(es) SMTP aparecerão como se fossem originadas do endereço especificado neste campo.
To address	O Nessus tentará enviar mensagens endereçadas ao destinatário da mensagem indicado neste campo. O endereço **postmaster** é o valor padrão, pois é um endereço válido na maioria dos servidores de correio.

“**SNMP settings**” (Configurações de SNMP) permite configurar o Nessus para se conectar e autenticar no serviço SNMP do destino. Durante a varredura, o Nessus fará algumas tentativas de descobrir o string da comunidade e usá-la em testes subsequentes. Até quatro strings de nomes de comunidades separadas podem ser usados por política de varredura. Se o Nessus não localizar o string e/ou a senha da comunidade, não poderá realizar uma auditoria completa do serviço.

Opção	Descrição
Community name (0-3)	O nome da comunidade SNMP.
UDP port	Instrui o Nessus a verificar uma porta diferente caso o SNMP esteja sendo executado em uma porta que não seja a porta 161.
SNMPv3 user name	O nome de usuário de uma conta que usa SNMPv3.
SNMPv3 authentication password	A senha do nome de usuário especificado.
SNMPv3 authentication algorithm	Selecione MD5 ou SHA1, dependendo do algoritmo reconhecido pelo serviço remoto.
SNMPv3 privacy password	A senha usada para proteger a comunicação SNMP criptografada.
SNMPv3 privacy algorithm	O algoritmo de criptografia a ser usado para o tráfego SNMP.

“**Service Detection**” (Detecção de Serviços) controla o modo como o Nessus testará serviços SSL: portas SSL conhecidas (por exemplo: 443), todas as portas ou nenhuma. O teste de funcionalidade SSL em todas as portas pode afetar o host verificado.

“**Unix Compliance Checks**” (Verificações de conformidade Unix) permite que os clientes do ProfessionalFeed enviem arquivos de auditoria do Unix que serão usado para determinar se um sistema testado cumpre as normas de conformidade especificadas. Até cinco políticas podem ser selecionadas ao mesmo tempo.

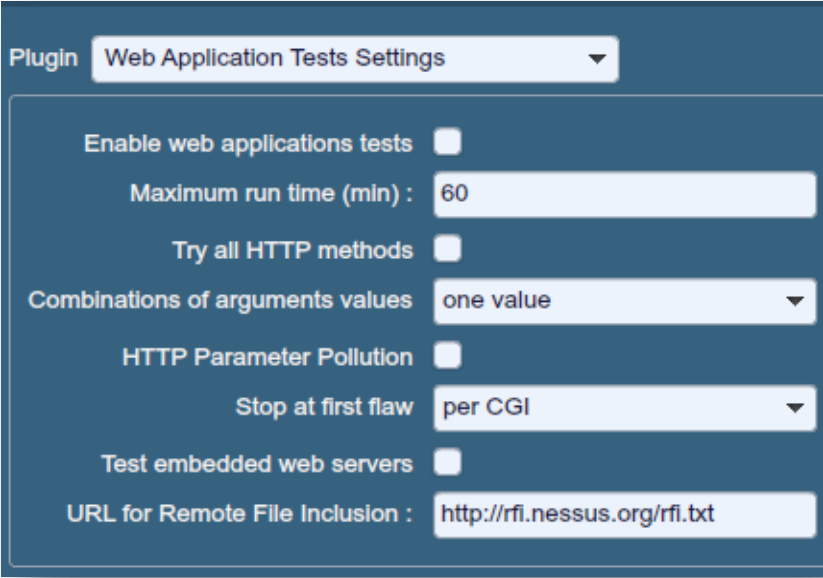
“VMware SOAP API Settings” (Configurações de API SOAP VMware) fornece as credenciais necessárias ao Nessus para autenticação dos sistemas de gerenciamento VMware ESX, ESXi e vSphere Hypervisor por meio do seu próprio API SOAP, uma vez que o acesso SSH foi descontinuado. O API foi projetado para auditoria de hosts do vSphere 4.x / 5.x, ESXi e ESX, mas não das máquinas virtuais em funcionamento nos hosts. Este método de autenticação pode ser usado para realizar varredura com credenciais ou auditorias de conformidade.

Opção	Descrição
VMware user name	Nome do usuário para autenticação. As credenciais podem ser contas do Active Directory (AD) (Diretório ativo) para hosts integrados ou contas locais e a conta deve estar no grupo `root` local. As credenciais de domínio são user@domain e as contas locais são usuário e senha.
VMware password (unsafe!)	Esta senha é enviada de forma insegura e pode ser interceptadas por meio de "sniffing" da rede.
Ignore SSL Certificate	Se um certificado SSL estiver presente no servidor, ignore-o.

“**Wake-on-LAN**” (Arranque remoto de LAN) controla os hosts que receberão pacotes "mágicos" WOL antes de realizar uma varredura, além do tempo de espera (em minutos) para a inicialização dos sistemas. A lista de endereços MAC do WOL é inserida por meio de um arquivo de texto enviado com um endereço MAC de host por linha. Por exemplo:

00:11:22:33:44:55
aa:bb:cc:dd:ee:ff
[…]

“**Web Application Tests Settings**” (Configurações dos Testes de Aplicativos de Web) verifica os argumentos das CGIs (Common Gateway Interfaces) remotas descobertas no processo de espelhamento de Web ao tentar enviar erros

comuns de programação de CGI, como cross-site scripting, inclusão remota de arquivos, execução de comandos, ataques transversais ou injeção de SQL. Ative esta opção marcando a caixa de seleção “Enable web applications tests” (Ativar testes de aplicativos da Web). Os testes dependem dos seguintes plugins NASL:

- 11139, 42424, 42479, 42426, 42427, 43160 – Injeção de SQL (abuso de CGI)
- 39465, 44967 – Execução de comandos (abuso de CGI)
- 39466, 47831, 42425, 46193, 49067 – Cross-Site Scripting (abuso de CGI: XSS)
- 39467, 46195, 46194 – Directory Traversal (abuso de CGI)
- 39468 – HTTP Header Injection (abuso de CGI: XSS)
- 39469, 42056, 42872 – Inclusão de arquivo (abuso de CGI)
- 42055- String de formato (abuso de CGI)
- 42423, 42054 - Server Side Includes (abuso de CGI)
- 44136 - Cookie Manipulation (abuso de CGI)
- 46196 - XML Injection (abuso de CGI)
- 40406, 48926, 48927 - Mensagens de erro
- 47830, 47832, 47834, 44134 - Ataques adicionais (abuso de CGI)

Nota: Esta lista de plugins relacionados a aplicativos da Web é atualizada com frequência e pode não ser completa. Os plugins adicionais podem depender das configurações desta opção de preferência.

Opção	Descrição
Maximum run time (min)	Esta opção gerencia o tempo (em minutos) usado na execução de testes de aplicativos da Web. O valor inicial desta opção é 60 minutos e se aplica a todas as portas e CGIs de um determinado website. A varredura de websites da rede local com aplicativos pequenos normalmente é realizada em menos de uma hora. No entanto, websites com aplicativos maiores podem exigir um valor maior.
Try all HTTP methods	Normalmente, o Nessus só irá realizar os teste com solicitações GET. Esta opção também instruirá o Nessus a usar “POST requests” para testes de formulários da Web aprimorados. Normalmente, os testes de aplicativos da Web usarão apenas solicitações GET, a menos que esta opção esteja ativada. Em geral, aplicativos mais complexos usam o método POST quando um usuário envia dados ao aplicativo. Esta configuração permite um teste mais completo, mas pode aumentar consideravelmente o tempo exigido. Se esta opção for selecionada, o Nessus testará cada script/variável com as solicitações GET e POST.
Combinations of arguments values	Esta opção gerencia a combinação de valores dos argumentos usados nas solicitações de HTTP. Este menu suspenso possui três opções: **one value** (Um valor)– Testa um parâmetro por vez com um string de ataque sem tentar variações de parâmetros adicionais “sem ataque”. Por exemplo: o Nessus tentaria aplicar “`/test.php?arg1=XSS&b=1&c=1`”, onde “`b`” e “`c`” permitem outros valores, sem testar cada combinação. Este é o método mais rápido de teste com o menor conjunto de resultados gerados.

	All pairs (Todos os pares) **(Mais lento mas eficiente)** – Esta forma de teste é um pouco mais lenta, mas é mais eficaz que o teste "one value". Ao verificar diversos parâmetros, verifica também o string de ataque, as variações de uma única variável e usa o primeiro valor com todas as outras variáveis. Por exemplo: o Nessus tenta aplicar "`/test.php?a=XSS&b=1&c=1&d=1`" e percorre as variáveis, de modo que uma receba o string de ataque e a outra redefina todos os valores possíveis (conforme descoberto durante o processo de espelhamento), e qualquer outra variável recebe o primeiro valor. Neste caso, o Nessus nunca testará "`/test.php?a=XSS&b=3&c=3&d=3`" quando o primeiro valor de cada variável for "`1`". **All combinations** (Todas as combinações) **(extremamente lento)** – Este método de teste realiza um teste completo de todas as combinações possíveis de sequências de ataque com entrada válida nas variáveis. Enquanto o teste "All-pairs" (Todos os pares) cria um conjunto menor de dados para maior desempenho, esta opção é bastante lenta, pois usa um conjunto completo de dados de testes. Esse método de teste pode levar muito tempo para ser concluído.
HTTP Parameter Pollution	Ao realizar testes de aplicativos da Web, esta opção tenta contornar qualquer mecanismo de filtragem por meio da injeção de conteúdo em uma variável enquanto fornece a mesma variável com conteúdo válido. Por exemplo: um teste de injeção SQL normal pode ter o seguinte aspecto: "`/target.cgi?a='&b=2`". Com a opção HTTP Parameter Pollution (HPP) ativada, a solicitação pode parecer a seguinte: "`/target.cgi?a='&a=1&b=2`".
Stop at first flaw	Esta opção determina um ataque em uma nova falha. Isto é feito no nível do script. A detecção de uma falha de XSS não desativará as pesquisas de injeção de SQL ou injeção de cabeçalho, mas haverá, no máximo, um relatório para cada tipo em uma determinada porta, a menos que "thorough tests" (testes completos) esteja definido. Observe que várias falhas do mesmo tipo (por exemplo: XSS, SQLI etc.) podem ser relatadas às vezes, se forem detectadas pelo mesmo ataque. O menu suspenso possui quatro opções: **per CGI** (por CGI) – Assim que uma falha é encontrada em uma CGI por um script, o Nessus passa à CGI conhecida seguinte no mesmo servidor ou, se não houver outras CGIs, à porta/servidor seguinte. Esta é a opção padrão. **per port** (por porta) **(mais rápido)**– Assim que uma falha é encontrada em um servidor Web por um script, o Nessus pára e alterna para o outro servidor Web em uma porta diferente. **per parameter** (por parâmetro) **(lento)**– Quando um tipo de falha é encontrado em um parâmetro de uma CGI (por exemplo: XSS), o Nessus alterna para o parâmetro seguinte da mesma CGI ou da CGI conhecida ou para a porta/servidor seguinte. **look for all flaws** (procurar todas as falhas) **(mais lento)**– Execute testes completos, independentemente das falhas encontradas. Esta opção pode gerar um relatório muito detalhado e, na maioria dos casos, não é recomendável.
Test Embedded web servers	Os servidores Web incorporados são, muitas vezes, estáticos e não contêm scripts de CGI personalizáveis. Além disso, os servidores da Web incorporados podem travar ou deixar de responder quando passam por uma varredura. A Tenable recomenda que os servidores Web incorporados sejam examinados separadamente de outros servidores Web com esta opção.
URL for Remote File Inclusion	Durante testes de inclusão remota de arquivos (RFI), esta opção especifica um arquivo em um host remoto para ser usado nos testes. Por padrão, o Nessus usará

	um arquivo seguro hospedado no servidor da Web da Tenable para os testes de RFI. Se o scanner não tiver acesso à Internet, recomenda-se usar um arquivo hospedado internamente para realizar testes mais precisos de RFI.

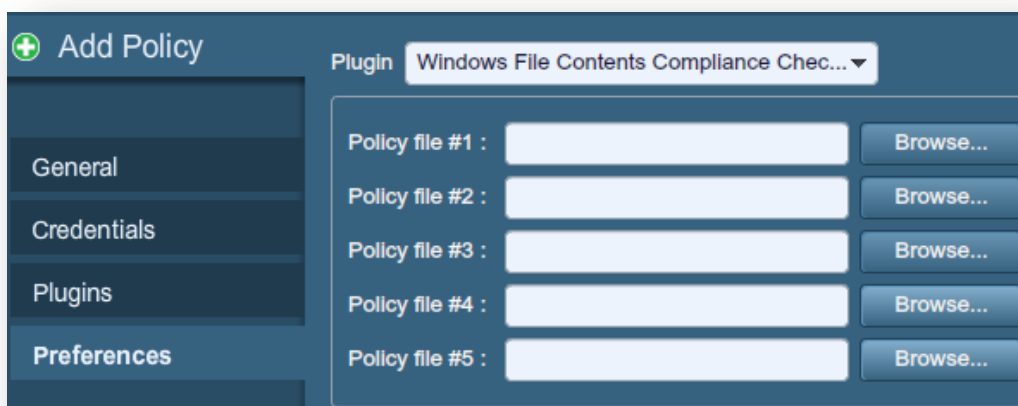
"**Web Mirroring**" (Espelhamento de Web) define os parâmetros de configuração para o utilitário original de espelhamento de conteúdo do servidor Web do Nessus. O Nessus realiza o espelhamento do conteúdo da Web para aprimorar a análise de vulnerabilidades e ajudar a reduzir o impacto sobre o servidor.

Se os parâmetros de espelhamento da Web forem definidos de maneira a espelhar um site inteiro, o aumento significativo do tráfego poderá ocorrer durante a varredura. Por exemplo: se houver 1 gigabyte de material em um servidor Web e o Nessus estiver configurado para espelhar todo o conteúdo, a varredura irá gerar pelo menos 1 gigabyte de tráfego do servidor para o scanner Nessus.

Opção	Descrição
Number of pages to mirror	Número máximo de páginas a espelhar.
Maximum depth	Limita o número de links que o Nessus seguirá em cada página inicial.
Start page	O URL da primeira página a ser verificada. Se forem necessárias várias páginas, use dois pontos para separá-las (por exemplo: "/:/php4:/base").
Excluded items regex	Permite que partes do website não estejam sujeitas ao rastreamento. Por exemplo: para excluir o diretório "/manual" e todas as CGIs Perl, defina esse campo como: `(^/manual)|(\.pl(\?.*)?$)`.
Follow dynamic pages	Se esta opção for selecionada, o Nessus seguirá os links dinâmicos e pode exceder os parâmetros definidos acima.

“**Windows Compliance Checks**” (Verificações de Conformidade de Windows) permite que os clientes do ProfessionalFeed enviem arquivos de auditoria do Microsoft Windows, que serão usados para determinar se um sistema testado cumpre as normas de conformidade especificadas. Até cinco políticas podem ser selecionadas ao mesmo tempo.

“**Windows File Contents Compliance Checks**” (Verificações de Conformidade do Conteúdo de Arquivos do Windows) permite que os clientes do ProfessionalFeed enviem arquivos de auditoria do Windows que pesquisam tipos específicos de conteúdos no sistema (por exemplo: cartões de crédito, números de documentos de identidade) para ajudar a determinar o cumprimento de normas internas da empresa ou normas externas.

Quando todas as opções forem configuradas da maneira desejada, clique em “**Submit**” (Enviar) para salvar a política e voltar à guia Políticas (Políticas). A qualquer momento, clique em “**Edit**” (Editar) para fazer alterações em uma política criada ou clique em “**Delete**” (Excluir) para excluir completamente uma política.

Para obter mais informações

A Tenable possui vários documentos que descrevem a instalação, implementação, configuração, operação do usuário e testes gerais do Nessus. O documentos estão listados a seguir:

- **Guia de Instalação do Nessus –** instruções passo a passo da instalação.
- **Verificações de Credenciais do Nessus para Unix e Windows –** informações sobre como realizar varreduras autenticadas de rede com o scanner de vulnerabilidades Nessus,
- **Verificações de Conformidade do Nessus –** guia geral para compreender e executar verificações de conformidade com o Nessus e o SecurityCenter.
- **Referência de Verificações de Conformidade do Nessus –** guia completo da sintaxe das verificações de conformidade do Nessus.
- **Formato de arquivo Nessus v2 –** descreve a estrutura do formato de arquivo `.nessus`, que foi introduzido com o Nessus 3.2 e NessusClient 3.2.
- **Especificação do protocolo Nessus XML-RPC –** descreve o protocolo e a interface XML-RPC do Nessus.
- **Monitoramento de Conformidade em Tempo Real –** descreve como as soluções da Tenable podem ser usadas para ajuda a cumprir muitos tipos diferentes de normas do governo e do setor financeiro.
- **Guia de administração SecurityCenter**

Outros recursos on-line são listados a seguir:

- Fórum de Discussão do Nessus: https://discussions.nessus.org/.
- Blog da Tenable: http://blog.tenable.com/
- Podcast da Tenable: http://blog.tenablesecurity.com/podcast/
- Vídeo de exemplos de uso: http://www.youtube.com/user/tenablesecurity
- Feed do twitter da Tenable: http://twitter.com/tenablesecurity

Entre em contato conosco pelo e-mail support@tenable.com, sales@tenable.com ou visite nosso site no endereço http://www.tenable.com/.

Sobre a Tenable Network Security

Tenable Network Security, líder em monitoramento unificado de segurança, é a criadora do scanner de vulnerabilidades Nessus e de soluções de primeira classe sem agente para o monitoramento contínuo de vulnerabilidades, pontos fracos de configuração, vazamento de dados, gerenciamento de logs e detecção de comprometimentos para ajudar a garantir a segurança da rede e o cumprimento das leis e normas FDCC, FISMA, SANS CSIS e PCI. Os produtos premiados da Tenable são utilizados por muitas organizações da Global 2000 e por órgãos públicos para tomar a iniciativa de reduzir os riscos nas redes. Para mais informações, visite http://www.tenable.com/.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com

Copyright © 2013. Tenable Network Security, Inc. Todos os direitos reservados. Tenable Network Security e Nessus são marcas comerciais registradas da Tenable Network Security, Inc.